

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-328846

(43)Date of publication of application : 15.11.2002

---

(51)Int.Cl. G06F 12/14  
G06F 17/60  
H04L 9/08  
H04L 9/32

---

(21)Application number : 2002-041890 (71)Applicant : SONY COMPUTER ENTERTAINMENT INC  
(22)Date of filing : 19.02.2002 (72)Inventor : SHIMADA SHUGI  
OKAMOTO SHINICHI  
YOSHIMORI MASAHARU  
INUI TSUTOMU  
SHIMAKAWA KEIZO  
OKADA TOYOJI  
KUBO AKIRA  
NAKAMURA MITSUHIRO

---

(30)Priority

Priority number : 2001044358 Priority date : 20.02.2001 Priority country : JP

---

(54) COPY MANAGEMENT SYSTEMCOMPUTER READABLE STORAGE MEDIUM IN WHICH INFORMATION PROCESSING PROGRAM OF CLIENT TERMINAL IS STOREDCOMPUTER READABLE STORAGE MEDIUM IN WHICH INFORMATION PROCESSING PROGRAM OF MANAGEMENT SERVER IS STOREDINFORMATION PROCESSING PROGRAM OF CLIENT TERMINALINFORMATION PROCESSING PROGRAM OF MANAGEMENT SERVERCOPY MANAGING METHODINFORMATION PROCESSING METHOD OF CLIENT TERMINAL AND INFORMATION PROCESSING METHOD OF MANAGING SERVER

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized copy of the contents.

SOLUTION: IDs (MIDs) are attached by every optical disk and the contents are encoded and recorded by a Content-Key. A system server manages a client ID of a client terminalan HDD-ID of an HDD and an MC-ID of a memory cardetc.owned by a user as user entry information. The user transmits the MC-ID to the system

server together with the MID of an optical disk when the contents are copied. The system server specifies the user by collating the MC-ID with the user entry information and returns the Content-Key used in the case of decoding the contents. The contents recorded in the optical disk is decoded and copied in the HDD by using the returned Content-Key on the user's side. Since copy of the contents is permitted only to a normal user as an owner of the storage medium the unauthorized copy of the contents is prevented.

---

## CLAIMS

---

[Claim(s)]

[Claim 1] A copy management system comprising:

A storage which contents enciphered with an enciphering key are memorized and peculiar medium identification information is attached and is distributed to a user from the administrator side.

When it has a copy function which decrypts contents memorized by the above-mentioned storage using a decryption key corresponding to the above-mentioned enciphering key and is copied to a secondary-storage medium and these contents are copied with medium identification information of the above-mentioned storage. A terminal unit of a user who transmits predetermined and peculiar device identification information.

A management server device which transmits a decryption key of the above-mentioned contents to a terminal unit of a user who has the above-mentioned device identification information when a medium identification number of the above-mentioned storage is received.

[Claim 2] A copy management system which is the copy management system according to claim 1 and is characterized by the above-mentioned management server device transmitting a decryption key once to one medium identification information.

[Claim 3] Are the copy management system according to claim 1 or 2 and the above-mentioned terminal unit identification information of the above-mentioned terminal unit identification information attached peculiar to a copy means which performs a copy of the above-mentioned contents And a copy management system combining any one or plurality among identification numbers attached peculiar to external semiconductor memory and transmitting as the above-mentioned device identification information.

[Claim 4] Are a copy management system given in any 1 paragraph among claim 1 to claims 3 and the above-mentioned management server device A copy management system decrypting and using a decryption key which the above-mentioned decryption key is enciphered it transmits by the above-mentioned device identification information and the above-mentioned terminal unit is the device identification information of self and was enciphered [ above-mentioned ].

[Claim 5] A copy management system which is a copy management system given in any 1 paragraph among claim 1 to claims 4 and is characterized by the above-mentioned terminal unit deleting the above-mentioned decryption key after decryption of the above-mentioned contents.

[Claim 6] Are a copy management system given in any 1 paragraph among claim 1 to claims 5 and the above-mentioned management server device Transmit and a re-enciphering key for re-enciphering the above-mentioned contents which copy the above-mentioned terminal unit A copy management system decrypting contents copied [ above-mentioned ] and reproducing using a re-enciphering key which re-enciphered copied contents decrypted with the above-mentioned decryption key with the above-mentioned re-enciphering key memorized the above-mentioned re-enciphering key to a memory measure and was memorized to the above-mentioned memory measure.

[Claim 7] Are a copy management system given in any 1 paragraph among claim 1 to claims 6 and the above-mentioned management server device Distribution management of the above-mentioned decryption key is performed by relating making it each user's device identification information and memorizing in a database medium identification information whose above-mentioned decryption key has been transmitted A copy management system rewriting old device identification information registered into the above-mentioned database to new device identification information when a user's device identification information is changed by repair or exchange.

[Claim 8] A copy management system which is a copy management system given in any 1 paragraph among claim 1 to claims 7 and is characterized by the above-mentioned management server device performing predetermined accounting to a user who has the terminal unit which transmitted a decryption key.

[Claim 9] Are a copy management system given in any 1 paragraph among claim 1 to claims 8 and mediate transmission and reception of information between the above-mentioned user's terminal unit and the above-mentioned management server device and. A copy management system having a mediation server device which performs accounting to a user when the above-mentioned decryption key is transmitted to a user's terminal unit at least.

[Claim 10] A storage characterized by comprising the following with which an information processing program of client terminal equipment was memorized and in which computer reading is possible.

A step which contents enciphered with an enciphering key are memorized and reads this medium identification information from a storage to which peculiar medium identification information was given.

A step which reads device identification information attached peculiar to a device used when a user copies the above-mentioned contents.

a step which transmits medium identification information and device identification information which carried out [ above-mentioned ] reading appearance at least to a server apparatus by the side of an administrator.

A step which receives a decryption key replied from a server apparatus by the

side of the above-mentioned administrator by transmitting the above-mentioned medium identification information and device identification informationA step which carries out decoding processing of the contents memorized by the above-mentioned storage using a decryption key which received [ above-mentioned ]and a step which copies contents which carried out [ above-mentioned ] decoding processing.

[Claim 11]A step which is the storage according to claim 10 and receives the above-mentioned decryption keyA step which receives a decryption key enciphered and transmitted by device identification information of a user's deviceand carries out decoding processing of the above-mentioned contentsA storage carrying out decoding processing of the contents which carry out decoding processing of the decryption key enciphered [ above-mentioned ]and are memorized by the above-mentioned storage by device identification information of a self device using this decryption key that carried out decoding processing.

[Claim 12]A storage which is the storage according to claim 10 or 11and is characterized by having a step which deletes the above-mentioned decryption key after a copy of the above-mentioned contents.

[Claim 13]A storage given [ among claim 10 to claims 12 characterized by comprising the following ] in any 1 paragraph.

A step which receives a re-enciphering key for re-enciphering the above-mentioned contents which copy transmitted from the above-mentioned management server device.

A step which re-enciphers and copies contents decrypted with the above-mentioned decryption key with the above-mentioned re-enciphering key.

A step which memorizes the above-mentioned re-enciphering key to a memory measure.

A step which decrypts contents copied [ above-mentioned ] using a re-enciphering key memorized by the above-mentioned memory measure when reproducing contentsand is reproduced.

[Claim 14]In a step which is a storage given in any 1 paragraph among claim 10 to claims 13and transmits the above-mentioned medium identification information and device identification information. Identification information attached peculiar as this device identification information to a terminal unit which a user usesA storage transmitting one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copiedor identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.

[Claim 15]A storage characterized by comprising the following with which an information processing program of a management server device was memorized and in which computer reading is possible.

A step which receives device identification information which is transmitted from a

user's device and which was attached peculiar to this device and medium identification information attached peculiar to a storage with which contents enciphered with an enciphering key were memorized.

A step which detects whether medium identification information which received [ above-mentioned ] is registered into a database with which medium identification information of a storage with which a copy of contents was performed is registered in the state where it was related with device identification information of each user's device.

A step which transmits a decryption key for decrypting the above-mentioned contents to a user's device when un-registering of the above-mentioned device identification information is detected.

[Claim 16] A storage which is the storage according to claim 15 and is characterized by having a step which relates medium identification information to which the above-mentioned decryption key was transmitted with a device identification number of a device of a user who performed this transmission and registers it into the above-mentioned database.

[Claim 17] A storage which it is the storage according to claim 15 or 16 and a step which transmits the above-mentioned decryption key is the device identification information of a user's device and is characterized by enciphering the above-mentioned decryption key and transmitting.

[Claim 18] A storage wherein a step which is a storage given in any 1 paragraph among claim 15 to claims 17 and transmits the above-mentioned decryption key transmits a re-enciphering key for re-enciphering the above-mentioned contents which copy.

[Claim 19] It is a storage given in any 1 paragraph among claim 15 to claims 18 A storage having a step which rewrites old device identification information registered into the above-mentioned database to new device identification information when new device identification information is given by repair or exchange to a user's device.

[Claim 20] A storage which is a storage given in any 1 paragraph among claim 15 to claims 19 and is characterized by having a step charged to a user who transmitted the above-mentioned decryption key.

[Claim 21] Are a storage of a statement given in any 1 paragraph among claim 15 to claims 20 and in the above-mentioned medium identification information and a step which carries out device identification information reception. Identification information attached peculiar as this device identification information to a terminal unit which a user uses A storage receiving one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copied or identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.

[Claim 22] An information processing program of client terminal equipment characterized by comprising the following.

A step which contents enciphered with an enciphering key are memorized and reads this medium identification information from a storage to which peculiar medium identification information was given.

A step which reads device identification information attached peculiar to a device used when a user copies the above-mentioned contents.

a step which transmits medium identification information and device identification information which carried out [ above-mentioned ] reading appearance at least to a server apparatus by the side of an administrator.

A step which receives a decryption key replied from a server apparatus by the side of the above-mentioned administrator by transmitting the above-mentioned medium identification information and device identification information  
A step which carries out decoding processing of the contents memorized by the above-mentioned storage using a decryption key which received [ above-mentioned ] and  
a step which copies contents which carried out [ above-mentioned ] decoding processing.

[Claim 23] A step which is the information processing program according to claim 22 and receives the above-mentioned decryption key  
A step which receives a decryption key enciphered and transmitted by device identification information of a user's device and carries out decoding processing of the above-mentioned contents  
An information processing program carrying out decoding processing of the contents which carry out decoding processing of the decryption key enciphered [ above-mentioned ] and are memorized by the above-mentioned storage by device identification information of a self device using this decryption key that carried out decoding processing.

[Claim 24] An information processing program which is the information processing program according to claim 22 or 23 and is characterized by having a step which deletes the above-mentioned decryption key after a copy of the above-mentioned contents.

[Claim 25] An information processing program given [ among claim 22 to claims 24 ] characterized by comprising the following ] in any 1 paragraph.

A step which receives a re-enciphering key for re-enciphering the above-mentioned contents which copy transmitted from the above-mentioned management server device.

A step which re-enciphers and copies contents decrypted with the above-mentioned decryption key with the above-mentioned re-enciphering key.

A step which memorizes the above-mentioned re-enciphering key to a memory measure.

A step which decrypts contents copied [ above-mentioned ] using a re-enciphering key memorized by the above-mentioned memory measure when reproducing contents and is reproduced.

[Claim 26] In a step which is an information processing program given in any 1 paragraph among claim 22 to claims 25 and transmits the above-mentioned medium

identification information and device identification information. Identification information attached peculiar as this device identification information to a terminal unit which a user uses. An information processing program transmitting one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copied or identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.

[Claim 27] An information processing program of a management server device characterized by comprising the following.

A step which receives device identification information which is transmitted from a user's device and which was attached peculiar to this device and medium identification information attached peculiar to a storage with which contents enciphered with an enciphering key were memorized.

A step which detects whether medium identification information which received [ above-mentioned ] is registered into a database with which medium identification information of a storage with which a copy of contents was performed is registered in the state where it was related with device identification information of each user's device.

A step which transmits a decryption key for decrypting the above-mentioned contents to a user's device when un-registering of the above-mentioned device identification information is detected.

[Claim 28] An information processing program which is the information processing program according to claim 27 and is characterized by having a step which relates medium identification information to which the above-mentioned decryption key was transmitted with a device identification number of a device of a user who performed this transmission and registers it into the above-mentioned database.

[Claim 29] An information processing program which it is the information processing program according to claim 27 or 28 and a step which transmits the above-mentioned decryption key is the device identification information of a user's device and is characterized by enciphering the above-mentioned decryption key and transmitting.

[Claim 30] An information processing program wherein a step which is an information processing program given in any 1 paragraph among claim 27 to claims 29 and transmits the above-mentioned decryption key transmits a re-enciphering key for re-enciphering the above-mentioned contents which copy.

[Claim 31] It is an information processing program given in any 1 paragraph among claim 27 to claims 30. An information processing program having a step which rewrites old device identification information registered into the above-mentioned database to new device identification information when new device identification information is given by repair or exchange to a user's device.

[Claim 32] An information processing program which is an information processing program given in any 1 paragraph among claim 27 to claims 31 and is characterized

by having a step charged to a user who transmitted the above-mentioned decryption key.

[Claim 33]Are an information processing program of a statement given in any 1 paragraph among claim 27 to claims 32and in the above-mentioned medium identification information and a step which carries out device identification information reception. Identification information attached peculiar as this device identification information to a terminal unit which a user usesAn information processing program receiving one of identification information or two or more identification information among identification information attached peculiar to a secondary memory with which the above-mentioned contents are copiedor identification information attached peculiar to a memory by which external is carried out to the above-mentioned terminal unit.

[Claim 34]When copying contents enciphered and memorized with an enciphering key with a user's device to which a peculiar device identification number was given by storage to which peculiar medium identification information was givenThe above-mentioned device identification information and the above-mentioned medium identification information are transmitted to a management server device from the above-mentioned deviceMedium identification information of a storage with which a copy of contents was performed in a database registered in the state where it was related with device identification information of each user's device. The above-mentioned management server device detects whether medium identification information transmitted from the above-mentioned user's device is registeredA copy management method which transmits a decryption key for decrypting the above-mentioned contents from the above-mentioned management server device to a user's device to the above-mentioned database when the above-mentioned medium identification information is unregistered.

[Claim 35]Contents enciphered with an enciphering key are memorizedand from a storage to which peculiar medium identification information was given. Read this medium identification information and device identification information attached peculiar to a device used when a user copies the above-mentioned contents is readby transmitting medium identification information and device identification information which carried out [ above-mentioned ] reading appearance at least to a server apparatus by the side of an administratorand transmitting the above-mentioned medium identification information and device identification information.An information processing method of client terminal equipment which carries out decoding processing of the contents which receive a decryption key replied from a server apparatus by the side of the above-mentioned administratorand are memorized by the above-mentioned storage using a decryption key which received [ above-mentioned ]and copies contents which carried out [ above-mentioned ] decoding processing.

[Claim 36]Device identification information which is transmitted from a user's device and which was attached peculiar to this deviceIn and the state where received medium identification information attached peculiar to a storage with which contents enciphered with an enciphering key were memorizedand it was



related with device identification information of each user's device. In a database with which medium identification information of a storage with which a copy of contents was performed is registered. An information processing method of a management server device which transmits a decryption key for decrypting the above-mentioned contents to a user's device when it detects whether medium identification information which received [ above-mentioned ] is registered and un-registering of the above-mentioned device identification information is detected.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention For example the storage with which the information processing program of a copy management system and client terminal equipment which performs copy management of computer programs such as game contents, movie contents, a music content and an application program was memorized and in which computer reading is possible. The information processing program of the storage with which the information processing program of the management server device was memorized and in which computer reading is possible and client terminal equipment, an information processing program of a management server device, a copy management method and an information processing method of client terminal equipment. And it is related with the information processing method of a management server device.

[0002]

[Description of the Prior Art] In today the video game machine which performs a video game based on the game contents memorized by storage such as CD-ROM, DVD-ROM or semiconductor memory has spread widely.

[0003] A user purchases the storage with which desired game contents were memorized, reproduces this storage with a video game machine and performs a video game. When the most the user buys and arranges a new video game gradually. For this reason the storage with which each game contents were memorized will be accumulated to the user with days and months.

[0004] However one reproducing mechanism of a storage is provided in the video game machine in many cases. For this reason when a different video game was performed the storage with which the video game machine is equipped now was taken out and very troublesome work [ say / newly reequipping with the storage with which the game contents which it will try to perform from now on were memorized ] was needed.

[0005]

[Problem(s) to be Solved by the Invention] This applicant is indicating the video game machine which made possible built-in or external [ of the mass hard disk drive (HDD) of tens of Order G (G) ] for example.

[0006]In the case of this video game machine the game contents memorized by each storage can be copied to HDD respectively and desired game contents can be reproduced and used from this HDD. By using this HDD the time and effort which detaches and attaches a storage to the reproducing mechanism of a video game machine is omissible.

[0007]Only the user who computer programssuch as game contents purchased here software with which the computer program was memorized and received justly is usable \*\*\*\*.

[0008]However when the copy of the computer program memorized by the storage is enabled at a secondary-storage medium we are anxious about the illegal copy which uses the computer program memorized by one storage for a secondary-storage medium in two or more users copying it respectively.

[0009]It is this invention's being made in view of an above-mentioned technical problem and performing copy management which enables the copy of a computer program only to a valid user. Prevention of an unauthorized use of contents etc. A storage with which the information processing program of the copy management system and client terminal equipment which were planned was memorized and in which computer reading is possible a storage with which the information processing program of the management server device was memorized and in which computer reading is possible an information processing program of client terminal equipment. It aims at offer of the information processing program of a management server device a copy management method the information processing method of client terminal equipment and the information processing method of a management server device.

[0010]

[Means for Solving the Problem] This invention attaches a peculiar identification number to a storage which made contents enciphered with an enciphering key memorize and distributes it to a user. An identification number is given also to a device used when a user copies contents.

[0011]When the above-mentioned device copies contents it transmits an identification number of the above-mentioned storage and an identification number of a device to a management server device. A management server device has the database with which an identification number of a device which each user uses was registered. A management server device compares an identification number of a device registered into a database and an identification number of a device transmitted from a user's device and specifies a user. A management server device transmits a decryption key for decrypting contents memorized by storage to a user's device when a user is specified by performing this collation.

[0012]A user's device decrypts contents memorized by the above-mentioned storage based on a decryption key distributed from this administrator side and copies contents.

[0013]A copy of contents can be permitted by this only to a regular user who is an owner of a storage and an illegal copy of contents can be prevented.

[0014]

[Embodiment of the Invention] This invention is applicable to the copy management system which performs copy management of a computer program.

[0015] As a computer program there are game contents, a music content, movie contents, an application program, etc. for example. As a storage with which the computer program was memorized, there is semiconductor memory besides optical disc, such as DVD-ROM and CD-ROM. As a secondary-storage medium used as the copy destination of a computer program, there are a hard disk (HD), DVD-RAM, a magneto-optical disc (MO), etc.

[0016] Hereafter, the above-mentioned game contents, a music content, movie contents, an application program, etc. are named generically and it is only considered as "contents."

[0017] [Entire configuration of a copy management system] The entire configuration of the copy management system used as a 1st embodiment of this invention is first shown in drawing 1. As shown in this drawing 1, the copy management system of this 1st embodiment has the client terminal equipment 1 provided with the regenerative function (execution function) of the contents memorized by the optical disc and the communication function through a network.

[0018] The hard disk drive 2 (HDD) for copying the contents memorized by the optical disc is connected to this client terminal equipment 1.

[0019] Communication MODEM 6 for aiming at connection with network, such as the Internet 5, is connected to this client terminal equipment 1.

[0020] Communication MODEM 6 may be formed in an external form to the client terminal equipment 1 as shown in this drawing 1. Communication MODEM 6 may be formed in the form of built-in in the client terminal equipment 1.

[0021] The copy management system has the system server device 4 provided with the database 3 with which user entry information was memorized.

[0022] The copy management system of this 1st embodiment comprises that this system server device 4 and the above-mentioned client terminal equipment 1 are mutually connected, for example via the network of Internet 5.

[0023] [Composition of client terminal equipment] The perspective view of the appearance of the client terminal equipment 1 is shown in drawing 2. This -- the controller terminal areas 7A and 7B and the memory card applied parts 8A and 8B are formed in the front-face side of the client terminal equipment 1 so that it may be shown figure 2.

[0024] To the front-face side of this client terminal equipment 1, the two USB contact buttons 9 to which the apparatus (USB: Universal Serial Bus) corresponding to USB is connected and the IEEE1394 contact button 10 which can respond, for example to the data transfer rate of a maximum of 400 Mbps(es) are formed.

[0025] The disk applied part 11 of the tray mold with which it is equipped with an optical disc is formed in the front-face side of this client terminal equipment 1.

[0026] The reset button 12 for resetting execution operation and reproduction motion of contents and the tray manual operation button 13 for operating receipts and payments of the tray of the optical disc applied part 11 are formed in the

front-face side of this client terminal equipment 1.

[0027]An electric power switchthe voice image output terminal (AV multi output terminal)the PC Card slotthe optical digital output terminalthe AC power input terminal etc. are provided in the back side of the client terminal equipment 1.

[0028]AV multi output terminal is connected to the television receiver 18 for a monitor via the AV cable 17. The video signal and audio signal which are outputted from the client terminal equipment 1 are supplied to the television receiver 18 for a monitor via this AV multi output terminal and the AV cable 17. Therebythe image of the above-mentioned contents is displayed on the television receiver 18. The sound of the above-mentioned contents is pronounced via the loudspeaker device of a television receiver.

[0029]The controller 14 is connected to the controller terminal areas 7A and 7B via the controller cable 15respectively.

[0030]The memory card applied parts 8A and 8B are equipped with the memory card for a save etc. which perform a save (memory) and read-out of game data.

[0031][Composition of a hard disk drive] Nextin drawing 2the case currently laid in the upper face part of the client terminal equipment 1 is the hard disk drive 2 (henceforth HDD2). This HDD2large hard diskssuch as 40 GBare provided in the inside. The game contents memorized by DVD-ROM for about ten sheets can be copied to this HDD2.

[0032]The power indicator 20 by which a lighting drive is carried outand the write-in indicator lamp 21 by which a lighting drive is carried out by being interlocked with the writing to a hard disk are formed in the power up at the front-face side of HDD2. The electric power switch and the data input/output terminal are provided in the back side of HDD2 at least.

[0033]A PC card is inserted in the above-mentioned PC Card slot provided in the back side of the client terminal equipment 1 when connecting HDD2 to the client terminal equipment 1. The end of a connecting cable is connected to a PC card in this state. The other end of a connecting cable is connected to the data input/output terminal of HDD2. Therebythe client terminal equipment 1 and HDD2 are electrically connected mutually.

[0034]In this exampleHDD2 is a different body in the client terminal equipment 1and we decided to carry out external to the client terminal equipment 1. Howeverthis HDD2 may be provided in the form built in the client terminal equipment 1.

[0035]It was presupposed that the client terminal equipment 1 and HDD2 are connected with a PC card via a connecting cable. Howevercontact buttonssuch as a USB contact button and an IEEE1394 contact buttonare provided in the back side (or it may be a front-face side.) of HDD2and it may be made to connect HDD2 to the client terminal equipment 1 via this contact button.

[0036][Electric constitution of client terminal equipment] Nextdrawing 3 is a block diagram of the client terminal equipment 1. As shown in this drawing 3the client terminal equipment 1 has CPU30the graphic processor 31 (GPU)and IO processor 32 (IOP).

[0037]The client terminal equipment 1 is provided with the following.  
The optical-disc-controlling part 33 which performs reproduction control of optical disc such as CD-ROM and DVD-ROM.  
Sound processor unit 34 (SPU).

[0038]The client terminal equipment 1 is provided with the following.  
MASK-ROM35 in which the operating system program which CPU30 and IOP32 execute was stored.  
RAM36 which functions as a buffer which stores temporarily the data read from the work area and optical disc of CPU30.

[0039]The client terminal equipment 1 has CD/DVDDSP38 which performs and outputs error correction processing (CIRC processing) etc. as opposed to the reproducing output from the optical disc supplied via RF amplifier 37 of the optical-disc-controlling part 33.

[0040]The client terminal equipment 1 has the driver 39 and the mechanical-completion troller 40 which perform the roll control of the spindle motor of the optical-disc-controlling part 33the focus/tracking control of an optical pickuploading control of a disk trayetc.

[0041]The client terminal equipment 1 has the card shape connector 41 to which the above-mentioned PC card is connected.

[0042]These each part is mainly mutually connected via the bus line 42 and 43 gradesrespectively.

[0043]Reproduction of the movie contents memorized by DVD-ROM is performed based on the DVD driver SOUFUTO wear memorized by the memory card. Or reproduction of movie contents is performed based on the DVD driver SOUFUTO wear printed on the semiconductor memory 44 (DVD Player ROM) built in in the client terminal equipment 1.

[0044]The operating system program is memorized by MASK-ROM35. CPU30 controls operation of the client-terminal-equipment 1 whole based on the operating system program memorized by this MASK-ROM35.

[0045]The hardware identification number (hardware ID) of the controller terminal areas 7A and 7Bthe memory card applied parts 8A and 8B and the controller 14 connected to the card shape connector 41the memory card 16and the HDD2 grade is also memorized by MASK-ROM35. Based on hardware ID memorized by this MASK-ROM35IOP32It communicates with the hardware of the controller 14the memory card 16and HDD2 gradeand the hardware connected to each contact buttons 7A7B8Aand 8B and card shape connector 41 grade is specified and recognized.

[0046]Hardware ID means ID generically attached to each hardware so to speak like one ID by one ID and the memory card 16 whole by the client-terminal-equipment 1 whole at one ID and the HDD2 whole.

[0047]On the other handclient IDMC-IDand HDD-ID which are mentioned later are every client terminal equipmentevery memory card 16and ID peculiar to each

hardware attached for every HDD2 respectively.

[0048] GPU31 is stored in the frame buffer which draws according to the drawing indication from CPU30 and does not illustrate the drawn picture. GPU31 has a function as a geometry transfer engine which processes coordinate conversion etc.

[0049] This GPU31 constitutes a virtual three-dimensional object from a set of the polygon of triangular shape when the game contents currently recorded for example on the optical disc use what is called 3D graphics. And GPU31 performs many calculations for generating the picture acquired by photoing this three-dimensional object with a virtual camera device. That is GPU31 performs transparent transformation processing in the case of performing a rendering (calculation of the coordinate value at the time of projecting the peak of each polygon which constitutes a three-dimensional object on a virtual camera screen) etc.

[0050] GPU31 draws to a frame buffer using a geometry transfer engine if needed according to the drawing indication from CPU30. And the video signal (visual out) corresponding to this picture that drew is outputted.

[0051] On the other hand SPU34 is reproducing the data point remembered to be the ADPCM function decoding which reproduces the voice data by which adaptive predictive coding was carried out by the sound buffer. It has the regenerative function which reproduces and outputs audio signals such as a sound effect (audio out) the abnormal-conditions function which is made to modulate the data point memorized by the sound buffer and is reproduced etc. This SPU34 operates as what is called a source of a sampling sound. SPU34 generates audio signals such as musical tone and a sound effect based on the data point memorized by \*\* Li and the sound buffer from CPU30 to directions.

[0052] As for such client terminal equipment 1 if a power supply is switched on CPU30 and IOP32 will read the operating system program for CPU30 and the operating system program for IOP32 from MASK-ROM35 respectively.

[0053] CPU30 controls each part of the client terminal equipment 1 by the operating system program for CPU30 in generalization. IOP32 controls input and output of the data between the controller 14 the memory card 16 and HDD2 grade by the operating system program for IOP32.

[0054] After CPU30 performs initialization processing such as operation confirming based on the operating system program for CPU30 it controls the optical-disc-controlling part 33 and carries out reproduction control of the contents currently recorded on the optical disc.

[0055] When the reproduced contents are game contents of a video game CPU30 According to the directions (command) from the player received from the controller 14 via IOP32 GPU31 and SPU34 are controlled and utterance of the display of the picture of game contents a sound effect musical tone etc. etc. is controlled.

[0056] When the reproduced contents are movie contents according to the directions from the player received from the controller 14 via IOP32 CPU30 controls GPU31 and SPU34 and controls the display of the image of movie contents audio utterance etc.

[0057][Copy management activities] Such a copy management system is managed as follows when the contents memorized by the optical disc are copied to HDD2.

[0058][Installation of an installer] First when this copy management system copies the contents memorized by the optical disc to HDD2 it needs to execute the application program for copy control (installer) with the client terminal equipment 1. In the case of this example the installer is memorized by the optical disc with contents. The client terminal equipment 1 installs an installer before copy \*\*\*\* of contents.

[0059] When installing an installer a user equips the client terminal equipment 1 with the optical disc in which the installer is memorized. If equipped with this optical disc CPU30 of the client terminal equipment 1 will read the installer memorized by the optical disc according to operation of a user's controller 14 automatically (auto run) and will carry out storage control of this to memory card 16 or RAM36.

[0060] The installer memorized by this memory card 16 or RAM36 is performed by CPU30 when a user specifies the copy of the contents memorized by the optical disc. CPU30 is performing this installer and performs copy control of contents.

[0061] An installer manufactures the optical disc in which only the installer was memorized by the system contractor side and it may be made to distribute this to a user. Or the memory card in which the installer was memorized by the system contractor side is manufactured and it may be made to distribute this to a user. In this case install work of an installer can be made omissible.

[0062] Or ROM the installer was remembered to be may be provided in the client terminal equipment 1. Even in this case install work of an installer can be made omissible.

[0063][Encryption of contents] Encryption processing is performed to the contents memorized by the optical disc using a symmetrical key (contents key: Content-Key) which is different for every contents as shown in drawing 4. "Media unique ID (media unique ID:MID)" which becomes peculiar for every optical disc besides the contents by which encryption processing was carried out in this way is memorized by the optical disc.

[0064][User registration] Next in the copy management system of this 1st embodiment when copying contents to HDD2 from an optical disc it registers for the system server device 4 as a user using "memory card ID (MC-ID)" given to each memory card 16 peculiar. The copy of contents is not permitted when this user registration is not performed.

[0065] Drawing 5 is a flow chart which shows a flow until a user registers as a user to the system server device 4. Drawing 6 is a mimetic diagram of the copy management system concerned in which the information transmitted and received by this user registration between the client terminal equipment 1 and the system server device 4 is shown.

[0066] User registration operation is explained using this drawing 5 and drawing 6. The flow chart of drawing 5 is started because a user switches on the main power of the client terminal equipment 1.

[0067] In Step S1 a user connects his own client terminal equipment 1 to the

system server device 4 via the Internet 5.

[0068]As shown in drawing 1specificallycommunication MODEM 6 for Internet connectivities is connected to this client terminal equipment 1 (or built-in). If an Internet connectivity is specified by the userCPU30 shown in drawing 3 will operate based on a predetermined WWW browserand will aim at establishment of the communication line between the client terminal equipment 1 concerned and the system server device 4 via this communication MODEM 6. Therebythe distance of this user registration progresses to Step S2.

[0069]The identification number (MC-ID) of the memory card in which the client terminal equipment 1 was equipped with CPU30 in Step S2The transmission control of the peculiar identification number (HDD-ID) attached for every peculiar identification number (client ID) attached for every client terminal equipment and HDD2 is carried out to the system server device 4.

[0070]If the communication line of the system server device 4 and the client terminal equipment 1 is establishedspecificallyCPU30 will communicate with the client terminal equipment 1HDD2and the memory card 16respectively. The identification number with which CPU30 was given to the client terminal equipment 1 by this communication peculiar (client ID)The identification number (HDD-ID) attached peculiar to HDD2 and the identification number (MC-ID) given to the memory card 16 with which the client terminal equipment 1 was equipped peculiar are acquiredrespectively.

[0071]CPU30 transmits these identification numbers to the system server device 4 sideas shown in drawing 6. Therebythe distance of this user registration progresses to Step S3.

[0072]Information is encipheredtransmitted and receivedfor example based on communications protocolssuch as SSL (Secure Sockets Layer)and communicative safety is secured between the client terminal equipment 1 and the system server device 4.

[0073]In this exampleCPU30 is communicating with each device and decided to acquire client IDHDD-IDand MC-IDand to transmit to the system server device 4 side. Howeverthe user is stuck on the client terminal equipment 1HDD2and the memory card 16 for client IDHDD-IDand MC-ID in the ability to be recognized visually at each caserespectively. For this reasonthis client IDHDD-IDand MC-ID are seenand a user operates the controller 14inputs each ID manuallyand may be made to transmit to the system server device 4 side.

[0074]Nextin Step S3the identification number (MC-ID) of the memory card in which the system server device 4 was transmitted by this user distinguishes whether it is effective ID. In this step S3this user registration distance progresses to step S4when MC-ID to which the system server device 4 was transmitted by the user distinguishes that it is effective IDand when it distinguishes that MC-ID transmitted by the user is invalid IDit progresses to Step S7.

[0075]Specificallythe system server device 4 has the database 3 which memorized client ID of all the client terminal equipment 1HDD-ID of all the HDD2and MC-ID of all the memory cards 16.



[0076]the system server device 4 -- the client terminal equipment 1 from a userHDD2and the memory card 16 -- eachif peculiar ID is transmittedFirstMC-ID which is peculiar ID of the memory card 16 transmitted by the userand each MC-ID registered into the database 3 are comparedand it is distinguished whether the same MC-ID as MC-ID of the memory card 16 transmitted by the user is registered into the database 3.

[0077]That isthe system server device 4 distinguishes whether MC-ID of the memory card 16 transmitted by the user is the same as MC-ID regularly registered into the database 3.

[0078]When MC-ID of the memory card 16 transmitted by the user is in agreement with neither of MC-ID regularly registered into the database 3as for the system server device 4access of this user registration is judged to be access of unjust user registration. In this casethe system server device 4 replies the message which refuses user registration of "being unable to register as a user in this memory card" to the client-terminal-equipment 1 side in Step S7 (invalid notice). By thisthis user registration distance will be completed in the form where user registration was interrupted.

[0079]When MC-ID of the memory card 16 transmitted by the user is in agreement with one which is regularly registered into the database 3 of MC-IDon the other handthe system server device 4In step S4the user ID (User ID) which is peculiar ID of the user who has accessed the system server device 4 is formed nowfor example using a random number etc.

[0080]And as shown in drawing 6the system server device 4 with the user's client IDHDD-IDand MC-ID. The user ID (User ID) which is the above-mentioned user's peculiar IDand MC-Key explained later are put togetherand it registers with the database 3 of the system server device 4 by making this into "user entry information."

[0081]Thusthe copy management system of the embodiment concerned specifies each user in the combination of three IDthe client terminal equipment 1 which each user ownsHDD2and the memory card 16and registers him into the database 3.

[0082]Since it is not possibleit can register by registering as a user based on these three ID that the client terminal equipment 1HDD2and three ID of the memory card 16 are altogether in agreement among different users as a user by certainly specifying a user. The illegal copy of the contents recorded on the optical disc mentioned later by this can be prevented more powerfully.

[0083]In the case of user registrationonly "MC-ID" and "client ID"It may be made to register as a user by transmitting "HDD-ID"MC-ID and client IDMC-ID and HDD-IDor "client ID and HDD-ID" to the system server device 4 side. not overlapping among different users in these casessince each ID is peculiar IDrespectively -- a user -- abbreviated \*\* -- it can register as a user by certainly specifying.

[0084]Nextwhen the distance of user registration progresses to Step S5the system server device 4As a proof which user registration completed regularlyuser

ID (User ID) is enciphered by MC-Key among the user entry information formed by the above-mentioned step S4 and this is replied to the client-terminal-equipment 1 side.

[0085][MC-Key] Here the above "MC-Key" is the key information for enciphering the information transmitted and received between the client terminal equipment 1 and the system server device 4. This MC-Key is beforehand memorized in the memory card 16 with MC-ID.

[0086]It is stuck on the case of the memory card 16 so that a user can recognize MC-ID visually but it is remembered in the memory card 16 that a user cannot recognize this MC-Key visually. This MC-Key has been the high information on confidentiality that neither a display nor an output is performed even when a user reproduces the information memorized in the memory card 16. For this reason this MC-Key cannot be recognized by user levels.

[0087]MC-Key memorized by each memory card 16 with MC-ID of all the memory cards 16 is memorized by the database 3 of the system server device 4. When MC-Key is needed read and refer to MC-Key for the system server device 4 from this database 3. For this reason MC-Key is not transmitted from the client terminal equipment 1 to the system server device 4.

[0088]Thus MC-Key has been the high information on confidentiality which cannot recognize and is not transmitted and received between the client terminal equipment 1 and the system server device 4 in user levels.

[0089]By making unnecessary transmission and reception of MC-Key between the client terminal equipment 1 and the system server device 4 MC-Key can prevent the inconvenience monitored by the third party.

[0090]When the system server device 4 replies user ID (User ID) it chooses MC-Key corresponding to a user's memory card 16 accessed now from MC-Key beforehand memorized by the database 3. And user ID (User ID) is enciphered using this selected MC-Key and it replies to the client terminal equipment 1.

[0091]This MC-Key is used when decrypting the above-mentioned user ID (User ID) media unique ID (media unique ID (MID)) a contents key (Content-Key) and Content-Gen-Key respectively.

[0092]MID is ID attached peculiar for every optical disc. A contents key is the encryption key used when carrying out encryption processing of the contents recorded on the optical disc. Content-Gen-Key is an encryption key used when performing re-encryption processing to the contents copied to HDD2.

[0093]The client terminal equipment 1 decrypts the contents played from the optical disc using the above-mentioned contents key. And the client terminal equipment 1 carries out re-encryption processing using above-mentioned Content-Gen-Key and copies these decrypted contents to HDD2. It mentions later in detail.

[0094]Next if user registration distance progresses to Step S6 the client terminal equipment 1 will carry out storage control of the user ID (User ID) replied from the system server device 4 side to the memory card 16. Thereby the complete process cycle of the user registration shown in the flow chart of this drawing 5 is

completed. And at this time the user ID (User ID) enciphered by MC-Key with MC-ID and MC-Key which are beforehand memorized as shown in drawing 6 will be memorized by the memory card 16.

[0095][Registration of media unique ID and acquisition of a contents key] Next only by lending the memory card 16 in which MC-ID, MC-Key and user ID (User ID) were recorded to other users if the copy of the contents currently recorded on the optical disc is enabled any number of times HDD2 it becomes possible to copy unjustly the contents currently recorded on the optical disc to other users' HDD and other users are not desirable things either.

[0096]When copying contents to HDD2 in the case of this copy management system a user transmits peculiar media unique ID (media unique ID (MID)) attached for every optical disc via the client terminal equipment 1 to the system server device 4 side. The system server device 4 registers media unique ID transmitted by the user and it transmits the contents key for decrypting the enciphered contents to a user. The client terminal equipment 1 decrypts the contents currently recorded on the optical disc using a contents key and copies them to HDD2. For this reason receiving this contents key means that the copy of contents was permitted from the system server device 4 to the client terminal equipment 1.

[0097]The system server device 4 transmits a contents key after checking that transmission of the contents key had not been performed in the past to media unique ID which received from the client terminal equipment 1.

Thereby transmission of the contents key to the same media unique ID can be restricted only at once.

[0098]For example after a certain user copies the contents memorized by the optical disc purchased by itself to his HDD2 suppose that this optical disc was lent to other users. When other users copy contents to HDD2 they transmit media unique ID of the lent optical disc to the system server device 4.

[0099]However the history which shows that transmission of the contents key was performed remains in the system server device 4 side to media unique ID of the optical disc. In this case distribution of a contents key does not perform the system server device 4 to other users. Other users who cannot obtain a contents key cannot copy contents to HDD2. This copy management system was carried out in this way and has prevented the illegal copy of contents.

[0100]A flow until registration and the user of media unique ID (MID) acquire a contents key to the flow chart of drawing 7 is shown. Each information transmitted and received between the client terminal equipment 1 and the system server device 4 in the case of acquisition of a contents key in the case of the registration of media unique ID to drawing 8 is shown.

[0101]Registration of media unique ID (MID) and the acquisition operation of a contents key are explained using this drawing 7 and drawing 8. The registration of media unique ID (MID) and the acquisition distance (registration acquisition distance) of a contents key which are shown in the flow chart of this drawing 7 are performed [ that the user is terminating the above-mentioned user registration regularly and ] as a premise.

[0102]Firstin Step S11the client terminal equipment 1 aims at establishment of the communication line between the system server devices 4. Therebythis registration acquisition distance progresses to Step S12.

[0103]In this examplethe communication line established between the client terminal equipment 1 and the system server device 4 after the above-mentioned end of user registration is once cutAt the time of execution of this registration acquisition distanceit is the explanation which establishes the communication line between the client terminal equipment 1 and the system server device 4 again.

[0104]Howeverit may be made to perform this registration acquisition distancewithout cutting the communication line established between the client terminal equipment 1 and the system server device 4 after the above-mentioned user registration. In this casethis registration acquisition distance will skip Step S11and will progress to Step S12 from a start.

[0105]Nextin Step S12the client terminal equipment 1 transmits the user ID (User ID) and MC-ID which were acquired as mentioned above to the system server device 4. The client terminal equipment 1 transmits media unique ID (MID) attached peculiar with this user ID and MC-ID to the optical disc in which the contents to be copied to HDD2 from now on were memorized to the system server device 4 side.

[0106]CPU30 communicates with the memory card 16and as shown in drawing 8specificallyit transmits MC-ID to the system server device 4 side. CPU30 reads the user ID enciphered by MC-Key as mentioned above from the memory card 16and transmits to the system server device 4 side. CPU30 enciphers media unique ID (MID) which controlled the optical-disc-controlling part 33 and was played from the optical disc by MC-Keyand transmits this to the system server device 4 side.

[0107]It may be made to transmit client ID and HDD-ID to the system server device 4 side with each of these information. Client ID and HDD-ID can be used for a user's specification with above-mentioned MC-ID. A user can be specified more correctly than the case where a user is specified only by MC-IDby specifying a user using three IDMC-IDclient IDand HDD-ID.

[0108]The information transmitted and received between the client terminal equipment 1 and the system server device 4 is encipheredtransmitted and receivedfor example based on communications protocolsuch as SSL (Secure Sockets Layer). Therebyhigh communication of safety can be performed between the client terminal equipment 1 and the system server device 4.

[0109]Nextin Step S13the user ID (User ID) to which the system server device 4 was transmitted from the client-terminal-equipment 1 side distinguishes whether it is effective ID. In this step S13when the system server device 4 distinguishes that user ID is effectivethis registration acquisition distance progresses to Step S14. On the other handin this step S13when the system server device 4 distinguishes that user ID is invalidthis registration acquisition distance progresses to Step S17.

[0110]Specificallythe system server device 4 reads MC-Key corresponding to this

MC-ID with reference to the database 3 based on MC-ID (and client IDHDD-ID) transmitted from the client-terminal-equipment 1 side. And the system server device 4 decrypts the user ID (User ID) and media unique ID (MID) which were enciphered and transmitted by MC-Key based on this MC-Key respectively.

[0111]As mentioned above user ID (User ID) MC-ID client IDHDD-ID etc. are memorized as user entry information by the database 3 by the side of the system server device 4. For this reason the system server device 4 searches User Information in the database 3 based on MC-ID (client ID and HDD-ID). And the system server device 4 compares the user ID (User ID) within this User Information and the user ID (User ID) of the user who is accessing the present system server device 4 side. The system server device 4 judges the user who is accessing the present system server device 4 side to be a regular user when above-mentioned both are in agreement. Thereby this registration acquisition distance progresses to Step S14.

[0112]The system server device 4 On the other hand the user ID (User ID) within User Information of the database 3 When the user ID (User ID) of the user who is accessing the present system server device 4 side is inharmonious it is judged that the user ID (User ID) is invalid. And the system server device 4 has [ in / Step S17 ] invalid "user ID. Please register as a user. The message which stimulates user registration of " etc. for the second time is replied to the client-terminal-equipment 1 side (invalid notice). This will be completed in the form where this registration acquisition distance was interrupted.

[0113]Next in Step S14 the contents currently recorded on the user's optical disc which the system server device 4 is accessing now distinguish whether there is any history copied in the past.

[0114]Specifically in the case of this copy management system all media unique ID (MID) given to each optical disc respectively is registered into the database 3. The system server device 4 leaves the history of a copy by setting a flag to media unique ID (MID) of the database 3 when the copy of contents is performed.

[0115]For this reason the system server device 4 will detect whether the flag stands to that media unique ID (MID) if media unique ID (MID) is decrypted. Thereby it can be distinguished whether the copy of contents was performed in the past from the optical disc which has the media unique ID (MID).

[0116]When the flag of the media unique ID (MID) does not stand it means that the copy of contents is not performed in the past from the optical disc to which the media unique ID (MID) was given. For this reason the system server device 4 sets the flag of that media unique ID (MID) in the database 3. The system server device 4 registers into that user's user entry information media unique ID (MID) which set this flag and advances this registration acquisition distance to Step S15.

[0117]On the other hand when the flag of the media unique ID (MID) stands it means that the copy of contents is performed from the optical disc to which the media unique ID (MID) was given in the past. For this reason the system server device 4 replies the message which refuses the copy of the contents of "being unable to copy contents from these media" to the client-terminal-equipment 1

side in Step S17 (invalid notice). This will be completed in the form where this registration acquisition distance was interrupted.

[0118]NextStep S15 is a step which progresses when the copy of contents is not performed from the user's optical disc in the past. In this case the system server device 4 enciphers the contents key (Content-Key) which enciphered the contents currently recorded on the optical disc using MC-Key of that user's memory card 16. And this enciphered contents key is transmitted to the client-terminal-equipment 1 side. Transmission of this contents key means that the copy of the contents currently recorded on the optical disc from the system server device 4 side to the user was permitted.

[0119]MC-Key is attached peculiar to the memory card 16 which the user owns. For this reason it can limit only to the user who has the memory card 16 in which that MC-Key was memorized in the user who can decrypt and use this contents key. Therefore the above-mentioned contents key can be safely transmitted only to a regular user.

[0120]The system server device 4 reads HDD-ID of the client's ID and HDD2 of the client terminal equipment 1 which the user is using based on the user entry information memorized by the database 3. It enciphers by "contents JIENKI (Content-Gen-Key)" which formed these each ID for example using the random number and the system server device 4 is replied to the client-terminal-equipment 1 side.

[0121]The system server device 4 enciphers by above-mentioned MC-Key and replies contents JIENKI (Content-Gen-Key) used when enciphering client ID and HDD-ID to the client-terminal-equipment 1 side.

[0122]Although explained later the client terminal equipment 1 compares client ID replied from the system server device 4 and client ID of the client terminal equipment 1 concerned. The client terminal equipment 1 compares HDD-ID transmitted from the system server device 4 and HDD-ID of HDD2 connected to the client terminal equipment 1 concerned. And two above-mentioned client ID and two above-mentioned HDD-ID check that it is in agreement respectively and the client terminal equipment 1 copies contents.

[0123]For this reason by replying client ID and HDD-ID which are beforehand registered from the system server device 4 to a user's client terminal equipment 1 the copy of contents can be enabled only in the user's client terminal equipment 1 and the combination of HDD2 which are beforehand registered into the database 3.

[0124]The system server device 4 enciphers contents JIENKI which enciphered client ID and HDD-ID using MC-Key given to the memory card 16 which the user owns peculiar and replies it to a user's client terminal equipment 1. It can limit only to the user who has the memory card 16 in which the MC-Key was memorized by this in the user who can decrypt and use contents JIENKI. Therefore above-mentioned contents JIENKI can be safely transmitted only to a regular user.

[0125]Next the contents key as which the client terminal equipment 1 was enciphered in Step S16 by MC-Key replied from the system server device 4 side

(Content-Key)Storage control of client ID and HDD-ID which were enciphered by contents JIENKI (Content-Gen-Key) enciphered by MC-Key and contents JIENKI (Content-Gen-Key) is carried out to the memory card 16respectively. Therebythe registration acquisition distance shown in the flow chart of this drawing 7 is completed.

[0126]Thusthis copy management system permits a copy of only the contents memorized by the optical disc which has media unique ID (MID) which did not have a copied history in the past. Therebythe copy of the contents memorized by each optical disc can be restricted at once. For this reasonthe third party to whom the optical disc in which the copy of contents was performed in the past was lent cannot copy contents from that lent optical disc. Thereforemany users can prevent the unauthorized use which copies contents from the optical disc of one sheet.

[0127][Copy of contents] Nexta user is acquiring this contents key (Content-Key)and it becomes possible to copy the contents currently recorded on the optical disc to HDD2.

[0128]The flow chart and drawing 10 which drawing 9 shows the flow of this copy distance are a figure showing typically the information dealt with between the client terminal equipment 1HDD2and the memory card 16when the copy of these contents is performed. The copy distance of contents is explained using this drawing 9 and drawing 10.

[0129]Firstthe flow chart of drawing 9 is started by ending registration of above-mentioned media unique IDand the user who acquired the contents key operating the client terminal equipment 1and specifying the copy of contents.

[0130]In Step S21IOP32 of the client terminal equipment 1 reads the contents key (Content-Key) and contents JIENKI (Content-Gen-Key) which were enciphered by MC-Keyrespectively from the memory card 16These are supplied to CPU30.

[0131]As mentioned aboveMC-Key is heldrespectively with the system server device 4 and this client terminal equipment 1. For this reasonCPU30 carries out decoding processing of the contents key (Content-Key) and contents JIENKI (Content-Gen-Key) which are enciphered [ above-mentioned ] using this MC-Key currently held. And CPU30 carries out storage control of this contents key and contents JIENKI that were decrypted to RAM36. Therebythis copy distance progresses to Step S22.

[0132]In Step S22IOP32 reads client ID and HDD-ID which were enciphered by contents JIENKI (Content-Gen-Key) from the memory card 16and supplies these to CPU30. CPU30 decrypts this client ID and HDD-ID using contents JIENKI (Content-Gen-Key) decrypted previously.

[0133]In this step S22CPU30 compares client ID which decrypted [ above-mentioned ]and client ID given to the client terminal equipment 1 concerned. CPU30 compares HDD-ID which decrypted [ above-mentioned ]and HDD-ID of HDD2 connected to the client terminal equipment 1 concerned.

[0134]Nextin Step S23CPU30 distinguishes whether each above-mentioned client ID and each above-mentioned HDD-ID are in agreementrespectively. When both

are in agreement this copy distance progresses to Step S24 that the copy of contents should be performed. When both are inharmoniousthis copy distance progresses to Step S28.

[0135]That client ID and HDD-ID which were decrypted from the memory card 16 are not in agreement with client ID of the client terminal equipment 1 and HDD-IDIt is shown that acquisition of the above-mentioned contents key (Content-Key) is not performed based on client-terminal-equipment [ of a regular user ] 1 and HDD2.

[0136]That isthe inaccurate user to whom the memory card 16 was lent from the registered user in this case shows that it is trying to copy contents.

[0137]For this reasonCPU30 carries out display control of the message which refuses the copy of the contents of "being unable to copy"for example to a user. By thisthis copy distance will be completed in the interrupted form.

[0138]NextStep S24 is a step which it performs when the client terminal equipment 1 detects coincidence of each above-mentioned client ID and each above-mentioned HDD-ID. In this caseCPU30 decrypts the contents played by the optical-disc-controlling part 33 from the optical disc using the contents key (Content-Key) memorized by RAM36. It re-enciphers by contents JIENKI (Content-Gen-Key) memorized by RAM36and CPU30 supplies these decrypted contents to HDD2.

[0139]Nextin Step S25HDD2 saves the contents re-enciphered by above-mentioned contents JIENKI as shown in drawing 10 at a hard disk (copy).

[0140]Nextat Step S26it is distinguished by CPU30 of the client terminal equipment 1 performing HDD2 and communication whether the copy of contents was completed. When the copy is not completedCPU30 is carrying out repeat execution control of the operation of the above-mentioned step S24 and Step S25and it supplies contents to HDD2 until the copy of contents is completed. Completion of the copy of contents will advance this copy distance to Step S27.

[0141]In Step S27since the copy of contents was completedIOP32 eliminates the contents key (Content-Key) memorized by the memory card 16. Therebythis copy distance is completed.

[0142]Thusthe contents which are enciphered by a contents key (Content-Key) and memorized by the optical disc are decrypted by the contents key published from the system server device 4and the client terminal equipment 1 copies them to HDD2. And the contents key (contents key published from the system server device 4) memorized in the memory card 16 is eliminated after the copy of these contents.

[0143]As mentioned abovein order that a copied history may remain in the database 3 to the optical disc in which the copy of contents was performed in the pastthe recurrence line of a contents key does not perform the system server device 4 in principle. For this reasonthe system server device 4 refuses the copy application from the third party to whom the optical disc in which the copy of contents was performed once was lent based on the copied history of the above-mentioned database. And the system server device 4 does not transmit a contents



key to this third party.

[0144]Since the above-mentioned third party cannot acquire a contents key he cannot decrypt the contents memorized by the lent optical disc. For this reason since contents cannot be decrypted even if the above-mentioned third party is able to copy contents to secondary-storage media such as HDD these contents cannot be used. Therefore this copy management system can prevent the unauthorized use of contents.

[0145][Reproduction of the copied contents] Next a user can be reincarnated repeatedly and can use now the contents copied to HDD2 in this way.

[0146]The flow chart which shows drawing 11 the flow of the reproduction distance of the contents saved HDD2 is shown. In this reproduction distance the mimetic diagram of the information dealt with between the client terminal equipment 1 HDD2 and the memory card 16 is shown in drawing 12.

[0147]The flow chart of drawing 11 is started because the user who terminated the copy of the above-mentioned contents regularly specifies reproduction of contents.

[0148]In Step S31 IOP32 of the client terminal equipment 1 reads contents JIENKI (Content-Gen-Key) enciphered by above-mentioned MC-Key from the memory card 16 and supplies this to CPU30. CPU30 decrypts this contents JIENKI using MC-Key currently held by the client-terminal-equipment 1 side and is reproduced.

[0149]Next in Step S32 IOP32 reads client ID and HDD-ID which were enciphered by contents JIENKI (Content-Gen-Key) from the memory card 16 and supplies this to CPU30. CPU30 decrypts this client ID and HDD-ID that were enciphered using contents JIENKI decrypted previously.

[0150]Next in Step S33 CPU30 compares client ID given to the client terminal equipment 1 concerned and client ID decrypted by above-mentioned contents JIENKI.

[0151]CPU30 compares HDD-ID of HDD2 connected to the client terminal equipment 1 concerned and HDD-ID decrypted by above-mentioned contents JIENKI.

[0152]That each above-mentioned client ID and each above-mentioned HDD-ID are not in agreement shows that HDD2 of other users' memory card 16 or other users' client terminal equipment 1 or other users is used. For this reason CPU30 displays the message which refuses reproduction of contents with "unreproducible" contents on a user in Step S35. By this the reproduction distance of these contents will be completed in the form interrupted.

[0153]Thus in this copy management system also when reproducing the contents copied to HDD2 collation of client ID and HDD-ID is performed. For example HDD2 where the memory card 16 which a regular user owns and contents were saved considers the case where it is lent to a third party. A third party will connect HDD2 with this lent memory card 16 to his own client terminal equipment and the contents memorized in this HDD2 will be reproduced.

[0154]However client ID memorized in the memory card 16 is a regular user's client ID. For this reason since client ID of a third party's client terminal equipment and

client ID memorized by the memory card 16 are not in agreement reproduction of the contents memorized by HDD2 is refused in a third party's client terminal equipment. For this reason even when memory card 16 and HDD2 is lent use of the contents copied to HDD2 can be prevented.

[0155] Next when each above-mentioned client ID and each above-mentioned HDD2 are in agreement respectively CPU30 decrypts the contents of HDD2 using contents JIENKI decrypted previously and memorizes this to RAM36. Thereby the reproduction distance of these contents is completed.

[0156] When the contents memorized by RAM36 are game contents of a video game for example CPU30 operates based on these game contents. And CPU30 carries out display control of the character of a video game for example and carries out pronunciation control of a sound effect BGM etc. Thereby the user can enjoy a video game based on the game contents copied to HDD2 from an optical disc.

[0157] When playing game contents directly from an optical disc and performing a video game whenever it performs a new video game the detaching work of an optical disc is required. However the detaching work of the optical disc which was needed whenever it performed a new video game is omissible by copying to HDD2 the game contents recorded on each optical disc in this way. For this reason the start of a new video game can be enabled smoothly.

[0158] Since the contents key memorized by the memory card 16 is eliminated after the copy of contents is completed from an optical disc the re-copy of contents cannot be performed. However contents JIENKI memorized by the memory card 16 is not eliminated even after the completion of a copy. For this reason the contents which were enciphered by contents JIENKI and copied to HDD2 are repeatedly decrypted using contents JIENKI memorized by this memory card 16 and are refreshable.

[0159] [Correspondence over repair of a device and exchange] Next in the case of this copy management system client ID HDD-IDMC-ID (collectively henceforth a device ID) etc. and user ID are put in block as user entry information and the system server device 4 manages them. However when the client terminal equipment 1 and the device of HDD2 grade are exchanged by breakage etc. the device ID of this exchanged device differs from the device ID registered as user entry information. Therefore when devices are exchanged in spite of being a regular user we are anxious about the copy and reproduction of contents becoming impossible using the exchanged device.

[0160] On the other hand in the case of this copy management system the unauthorized use of contents is prevented by securing the indigence of a device ID. For this reason even when repair restores the client terminal equipment 1 and the device of HDD2 grade the device after this repair is received it is preferred to attach a different new device ID from the device ID attached before repair to distinguish the device before repair and the device after repair clearly and to manage them.

[0161] However like the time of exchange of the above-mentioned device if a new device ID is attached to the device after repair in this way in spite of being a

regular user we will be anxious about the copy and reproduction of contents becoming impossible using the fixed device.

[0162] This copy management system has prevented as follows the above-mentioned inconvenience about which we are anxious by using a new device ID by repair and exchange of a device.

[0163] [Correspondence over repair of client terminal equipment and HDD and exchange] The mimetic diagram for explaining the correspondence over repair of the client terminal equipment in this copy management system and HDD and exchange is shown in drawing 13. Client-terminal-equipment 1 or HDD2 on which x seal is drawn shows the damaged device among this drawing 13.

[0164] In this drawing 13 when a device is damaged a user sends that damaged device to the repair center by the side of the administrator who manages this copy management system with the memory card 16.

[0165] Namely although the memory card 16 is not damaged in this case Client ID and HDD-ID (each ID is hereafter called device ID collectively) which were enciphered by contents JIENKI (Content-Gen-Key) or contents JIENKI (Content-Gen-Key) are memorized by the memory card 16. For this reason even when a device is damaged the memory card 16 is sent to the above-mentioned repair center with this damaged device (or carrying in).

[0166] In a repair center if the broken device is sent it will fix and exchange so that this device may operate normally and a new device ID is given to devices carried out such as this repair and exchange.

[0167] Specifically client ID of the client terminal equipment 1 is memorized by MASK-ROM35 for example with above-mentioned hardware ID and an operating system program. The same MASK-ROM as the above-mentioned MASK-ROM35 is provided also in HDD2 and HDD-ID is memorized by this MASK-ROM. For this reason in a repair center when a device is fixed, MASK-ROM provided before performing this repair is removed and grant of new client ID or HDD-ID is performed by exchanging for MASK-ROM new client ID or HDD-ID was remembered to be.

[0168] Since a different device ID from the device broken in MASK-ROM of this new device is memorized when exchanging the device itself for a new device exchange of MASK-ROM like [ at the time of the above-mentioned repair ] is not performed.

[0169] Next the operator of a repair center reproduces MC-ID of the memory card 16 sent with the broken device. An operator accesses the database 3 of the above-mentioned system server device 4 via the terminal unit formed in the repair center and refer to the user entry information memorized by the above-mentioned database 3 for it based on MC-ID reproduced from the above-mentioned memory card 16. And an operator operates a terminal unit and carries out correction registration of the device ID among the user entry information memorized by this database 3 at the newly given device ID. An operator operates the database 3 via a terminal unit and takes down the above-mentioned flag set to copied contents.

[0170] Contents JIENKI (Content-Gen-Key) which an operator operates a terminal

unit and is memorized in the memory card 16 and which was enciphered by MC-Key. The device ID (client ID and HDD-ID) enciphered by contents JIENKI (Content-Gen-Key) is eliminated respectively. And this memory card 16 is returned to a user with the exchanged device [fix and] (or personal delivery).

[0171] By this the state of a user's device (the client terminal equipment 1, HDD2 and memory card 16) will return to the state (state just before copying = contents) immediately after completing the user registration distance explained using drawing 5 and drawing 6.

[0172] The user to whom this memory card 16 and device were returned operates the client terminal equipment 1 so that registration of media unique ID (MID) explained using drawing 7 and drawing 8 and acquisition of a contents key (Content-Key) may be performed again.

[0173] The client terminal equipment 1 accesses the system server device 4 corresponding to a user's operation and registers media unique ID (MID). And the client terminal equipment 1 re-copies to HDD2 the contents memorized by the optical disc using the contents key (Content-Key) acquired from the system server device 4 by this registration.

[0174] Thereby if it is a regular user even when repair and exchange of a device newly give a device ID, execution of the copy and reproduction of contents can be enabled based on a new device ID.

[0175] In the copy management system side by attaching a new device ID to the device restored by repair or exchange, the device before repair and the device after repair can be distinguished clearly and can be managed.

[0176] [Correspondence over breakage of a memory card and loss] Next in the case of this copy management system to breakage of the memory card 16 or loss it is coped with as follows. The mimetic diagram for explaining the correspondence over breakage of the memory card 16 in this copy management system and loss is shown in drawing 14. The memory card 16 surrounded and shown by the frame of a dotted line shows the memory card 16 damaged or lost among this drawing 14.

[0177] When the memory card 16 is damaged or lost as shown in this drawing 14a a user connects the client terminal equipment 1 to the system server device 4 via the Internet 5 and applies for the recurrence line of a memory card to the system server device 4.

[0178] If this application is made the system server device 4 will transmit the input screen data of user ID to the client-terminal-equipment 1 side. Thereby a user's client terminal equipment 1 carries out display control of the input screen of user ID to the television receiver 18.

[0179] A user inputs user ID to this input screen. However since the memory card 16 is damaged or lost in this case user ID (User ID) cannot be read from the memory card 16. For this reason a user inputs user ID seeing the user ID copied into the memo pad etc. when user ID is published. The client terminal equipment 1 transmits this inputted user ID to the system server device 4.

[0180] Next refer to the user entry information corresponding to the user ID transmitted by this user for the system server device 4 from the database 3.

Thereby the system server device 4 can recognize the contents etc. which were copied with contents JIENKI (Content-Gen-Key) or its memory card 16 with MC-ID and MC-Key of the memory card 16 which were damaged or lost.

[0181] Next the system server device 4 receives memory card 16new which has new MC-ID New MC-Key (New-MC-Key) and contents JIENKI (Content-Gen-Key) newly enciphered by this New-MC-Key. Client ID and HDD-ID which were enciphered by this contents JIENKI (Content-Gen-Key) are rerecorded. The system server device 4 rewrites MC-ID MC-Key etc. so that the user entry information memorized by the database 3 may turn into user entry information corresponding to this new memory card 16new.

[0182] It is a case where the memory card 16 is damaged or lost in this case and client-terminal-equipment [ of a user ] 1 and HDD2 is operating normally. For this reason as client ID enciphered by contents JIENKI (Content-Gen-Key) and HDD-ID the original device ID is used as it is.

[0183] Next a repair center sends this memory card 16new to the user side physically for example by mail etc. As mentioned above in the system server device 4 side the user entry information of the database 3 is rewritten with rewriting of each information in this memory card 16new. For this reason the user who received sent memory card 16new can perform copy of contents copied reproduction of contents etc. like before using this memory card 16new the client terminal equipment 1 and the system of the combination of HDD2.

[0184] [Effect of a 1st embodiment] The copy management system of this 1st embodiment stores the contents to which the system administrator performed encryption processing by the contents key in the optical disc in which media unique ID (MID) was given and is distributed to a user so that clearly from the above explanation.

[0185] When a user copies contents she transmits MID of an optical disc to the system server device 4. A user transmits the device IDs (client ID HDD-ID MC-ID etc.) of the device which he is using to the system server device 4.

[0186] The system server device 4 was related with the device ID of the device which each user is using and MID of the optical disc in which the copy of contents was performed in the past is memorized in the database 3.

[0187] MID of the device ID and optical disc in which the user is using the system server device 4 when the copy application of contents is made from a user -- it is based and the database 3 is referred to. The system server device 4 transmits the contents key for decrypting contents on condition that the MID same in the database 3 is not registered to a user's client terminal equipment 1.

[0188] The client terminal equipment 1 decrypts the contents memorized by the optical disc using this contents key and copies them to HDD2.

[0189] When this copy management system puts up the same MID as MID registered into the database 3 and a copy application is made distribution of the above-mentioned contents key is not performed. For this reason this copy management system can restrict the copy of contents at once and can prevent the illegal copy of contents.

[0190][A 2nd embodiment] The copy management system which serves as a 2nd embodiment of this invention next is explained. The copy management system of a 1st above-mentioned embodiment registers as a user by a user connecting his own client terminal equipment 1 to the system server device 4 by the side of a system administrator directly acquires a contents key (Content-Key) etc. and copies contents.

[0191]The 3rd person management server device with which the 3rd person manages the copy management system of this 2nd embodiment between a user's client terminal equipment 1 and the system server device 4 by the side of a system administrator is formed. A user acquires a contents key (Content-Key) etc. via this 3rd person management server device. The 3rd person management server device performs fee collection to offer of this contents key (Content-Key).

[0192][Composition of a 2nd embodiment] The system configuration figure of the copy management system used as this 2nd embodiment is shown in drawing 15. When this drawing 15 copies contents from an optical disc it shows the flow which acquires a contents key (Content-Key).

[0193]As for the system server device 4 and the 3rd person management server device 50 in this drawing 15 the dedicated line and the public line are mutually connected by available VPN (Virtual Private Network) etc. like a dedicated line for example.

[0194]The system server device 4 is not connected to the Internet 5 but this 3rd person management server device 50 is connected to the Internet 5. For this reason the user cannot access directly to the system server device 4 but will access the system server device 4 indirectly via this 3rd person management server device 50.

[0195][Operation of a 2nd embodiment] Next explanation of the copy management system of this 2nd embodiment of operation is given. In the case of the copy management system of this 2nd embodiment the user who tries to copy contents connects his own client terminal equipment 1 to the 3rd person management server device 50 via the Internet 5 from an optical disc. And a user transmits MC-ID (User ID) and media unique ID (MID) to the 3rd person management server device 50 side via the client terminal equipment 1. A user transmits the account information for 3rd person management server device 50 (for example a user name, a password etc.) to the 3rd person management server device 50 via the client terminal equipment 1.

[0196]The client terminal equipment 1 transmits MC-ID and account information to the 3rd person management server device 50 as it is. The client terminal equipment 1 enciphers user ID (User ID) and media unique ID (MID) of an optical disc by MC-Key and transmits these to the 3rd person management server device 50.

[0197]The 3rd person management server device 50 extracts and acquires account information among each information transmitted from the client terminal equipment 1. The 3rd person management server device 50 transmits the user ID (User ID) enciphered by MC-ID and MC-Key via the dedicated line (or the above-

mentioned VPN) and media unique ID (MID) enciphered by MC-Key to the system server device 4.

[0198] If this MC-ID, user ID and MID are received, the system server device 4 transmits the contents key (Content-Key) for decrypting the contents which are similarly enciphered as the above-mentioned and are recorded on the optical disc is enciphered by MC-Key and it replies to the 3rd person management server device 50. The system server device 4 enciphers contents JIENKI (Content-Gen-Key) by MC-Key and replies it to the 3rd person management server device 50. Furthermore, the system server device 4 enciphers a user's client ID and HDD-ID by this contents JIENKI (Content-Gen-Key) and replies them to the 3rd person management server device 50.

[0199] The contents key as which the 3rd person management server device 50 was enciphered by this MC-Key (Content-Key), contents JIENKI enciphered by MC-Key (Content-Gen-Key) and a user's client ID enciphered by contents JIENKI (Content-Gen-Key) and HDD-ID are transmitted to a user's client terminal equipment 1 via the Internet 5 respectively.

[0200] The 3rd person management server device 50 performs fee collection to the user based on the account information for 3rd person management server device 50 previously transmitted from the client terminal equipment 1 in compensation for having provided the contents key (Content-Key).

[0201] The client terminal equipment 1 carries out storage control of the above-mentioned contents key transmitted from the 3rd person management server device 50, contents JIENKI, client ID and HDD-ID to the memory card 16 and uses them for reproduction of the contents which are copied and copied as mentioned above.

[0202] The number of a user's credit card and the amount information by which prepaid one was carried out are beforehand registered into the 3rd person management server device 50 side, for example. For this reason, a credit card company is asked for the amount of money charged in exchange for offer of a contents key and the 3rd person management server device 50 collects it. Or the 3rd person management server device 50 subtracts and collects the charged amount of money from the balance by which prepaid one is carried out.

[0203] For example, between the administrator of the system server device 4 and the administrator of the 3rd person management server device 50, the money collected in this way will be distributed at a predetermined rate.

[0204] [Effect of a 2nd embodiment] The copy management system of this 2nd embodiment forms and constitutes the 3rd person management server device 50 between the client terminal equipment 1 and the system server device 4 in this way. A user accesses the system server device 4 via this 3rd person management server device 50 and charges distribution of a contents key (Content-Key). The 3rd person management server device 50 is charged by distributing this contents key (Content-Key) to a user.

[0205] Thereby, this copy management system can provide a new copy management system called the copy management system with which the 3rd person

(administrator of the 3rd person management server device 50) intervenes and also can acquire the same effect as the copy management system of a 1st above-mentioned embodiment.

[0206]Contents can be distributed gratuitously to a user via a predetermined network via an optical disc etc. by charging it when this copy management system distributes a contents key to a user.

[0207]In this copy management system when a user is supplied widely and there is an application of a copy from a user without giving MID to an optical disc the system server device 4 or the 3rd person management server device 50 may be made to charge by distributing a contents key to that user.

[0208]Although it is presupposed that the 3rd person management server device 50 charges the copy management system of this 2nd embodiment the system server device 4 may be made to charge this.

[0209]Finally this invention is not limited to each above-mentioned embodiment described as an example. For this reason if it is a range which does not deviate from the technical idea concerning this invention even if it is except each above-mentioned embodiment of course according to a design etc. various change is possible.

[0210]For example in explanation of each above-mentioned embodiment it was presupposed to the client terminal equipment 1 as device identification information that client ID, HDD-ID and MC-ID are transmitted to the system server device 4. However only client ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarly only HDD-ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarly only MC-ID may be transmitted to the system server device 4 from the client terminal equipment 1.

[0211]Client ID and HDD-ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarly client ID and MC-ID may be transmitted to the system server device 4 from the client terminal equipment 1. Similarly HDD-ID and MC-ID may be transmitted to the system server device 4 from the client terminal equipment 1.

[0212]That is the copy management system of each above-mentioned embodiment prevents an illegal copy by associating the storage with which the copy of contents is performed and the device used for the copy of contents and performing copy management by the system server device 4 side. For this reason as device identification information transmitted to the system server device 4 from the client terminal equipment 1 what is necessary is just the identification information which can specify a user.

[0213]Although we decided to use the memory card 16 in explanation of each above-mentioned embodiment when it is this copy management system the memory card 16 is not necessarily needed. What is necessary is just to make the memory built in HDD2 or the client terminal equipment 1 memorize the above-mentioned contents key memorized by the memory card 16 contents JIENKI etc. when not using the memory card 16.



[0214]

[Effect of the Invention] This invention can permit the copy of the contents memorized by the storage only to the regular user who is an owner of a storage. For this reason the illegal copy of the contents memorized by the storage can be prevented.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram showing the system configuration of the copy management system of a 1st embodiment of this invention.

[Drawing 2] It is a perspective view showing the appearance of the client terminal equipment which constitutes a copy management system and a hard disk drive (HDD).

[Drawing 3] It is a block diagram showing the electric composition of client terminal equipment.

[Drawing 4] It is the figure for explaining the optical disc used for this copy management system with which the digital contents enciphered by the contents key (Content-Key) were memorized.

[Drawing 5] It is a flow chart which shows the flow of the user registration in a copy management system.

[Drawing 6] It is a mimetic diagram of the copy management system in which each information transmitted and received between client terminal equipment and a system server device at the time of user registration is shown.

[Drawing 7] It is a flow chart which shows the register operation of media unique ID (MID) in a copy management system individually given to the optical disc and the acquisition operation of a contents key (Content-Key).

[Drawing 8] It is a mimetic diagram of the copy management system in which each information transmitted and received between client terminal equipment and a system server device at the time of registration of media unique ID (MID) individually given to the optical disc and acquisition of a contents key (Content-Key) is shown.

[Drawing 9] It is a flow chart which shows the flow of the copy distance in a copy management system.

[Drawing 10] It is a mimetic diagram showing each information transmitted and received between client terminal equipment, a memory card, and a hard disk drive at the time of copy execution.

[Drawing 11] It is a flow chart which shows the reproduction motion of the digital contents copied to the hard disk drive in a copy management system.

[Drawing 12] It is a mimetic diagram showing the information transmitted and received between client terminal equipment, a memory card, and a hard disk drive at the time of reproduction of the digital contents copied to the hard disk drive.

[Drawing 13] It is a mimetic diagram for explaining correspondence of the copy

management system to repair or exchange of client terminal equipment or a hard disk drive.

[Drawing 14] It is a mimetic diagram for explaining correspondence of the copy management system to breakage or loss of a memory card.

[Drawing 15] At the time of registration of media unique ID (MID) individually given to the optical disc. And it is a mimetic diagram of the copy management system used as a 2nd embodiment of this invention showing each information transmitted and received between client terminal equipment and a system server device at the time of acquisition of a contents key (Content-Key).

[Description of Notations]

1 [ -- A system server device 5 / -- The Internet 6 / -- Communication  
MODEM ] -- Client terminal equipment 2 -- A hard disk drive (HDD) 3 -- A  
database 4

---

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-328846  
(P2002-328846A)

(43) 公開日 平成14年11月15日 (2002. 11. 15)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
			3 2 0 F 5 J 1 0 4
17/60	1 4 2	17/60	1 4 2
	3 0 2		3 0 2 E
	3 3 2		3 3 2

審査請求 有 請求項の数18 O L (全 28 頁) 最終頁に続く

(21) 出願番号 特願2002-41890 (P2002-41890)  
(22) 出願日 平成14年2月19日 (2002. 2. 19)  
(31) 優先権主張番号 特願2001-44358 (P2001-44358)  
(32) 優先日 平成13年2月20日 (2001. 2. 20)  
(33) 優先権主張国 日本 (J P)

(71) 出願人 395015319  
株式会社ソニー・コンピュータエンタテインメント  
東京都港区赤坂7-1-1  
(72) 発明者 島田 宗毅  
東京都港区赤坂7丁目1番1号 株式会社  
ソニー・コンピュータエンタテインメント  
内  
(74) 代理人 100107238  
弁理士 米山 尚志

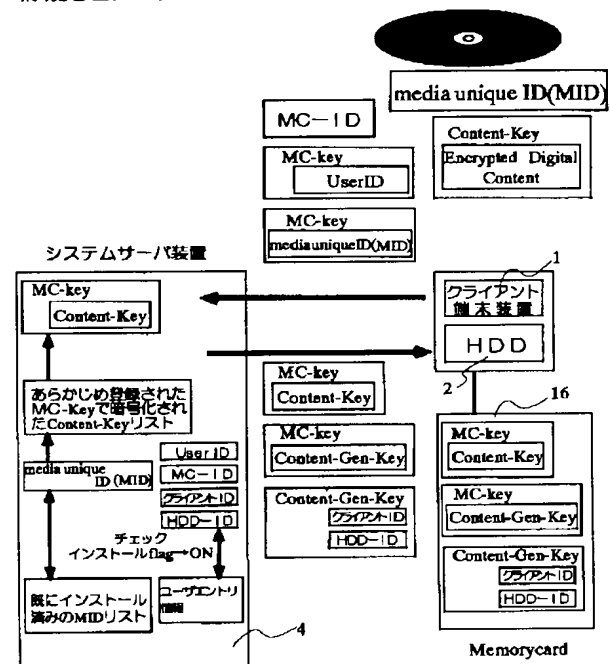
最終頁に続く

(54) 【発明の名称】 コピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体

(57) 【要約】

【課題】 コンテンツの不正コピーを防止する。

【解決手段】 各光ディスク毎にID (MID) を付すと共に、コンテンツをContent-Keyで暗号化して記録しておく。システムサーバ装置は、ユーザが所有するクライアント端末装置のクライアントID、HDDのHDD-ID、及びメモ리카ードのMC-ID等をユーザエントリ情報として管理する。ユーザはコンテンツのコピーを行う際に、光ディスクのMIDと共にMC-IDをシステムサーバ装置に送信する。システムサーバ装置は、MC-IDをユーザエントリ情報と照合してユーザを特定し、コンテンツの暗号化の際に用いたContent-Keyを返送する。ユーザ側では、この返送されたContent-Keyを用いて光ディスクに記録されているコンテンツを復号化しHDDにコピーする。記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーが許可されるため、コンテンツの不正コピーを防止することができる。



## 【特許請求の範囲】

【請求項1】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付され、管理者側からユーザに配布される記憶媒体と、

上記記憶媒体に記憶されているコンテンツを、上記暗号化鍵に対応する復号化鍵を用いて復号化して二次記憶媒体にコピーするコピー機能を有し、該コンテンツのコピーを行う際に、上記記憶媒体の媒体識別情報と共に、所定かつ固有のデバイス識別情報を送信するユーザの端末装置と、

上記記憶媒体の媒体識別番号を受信した際に、上記デバイス識別情報を有するユーザの端末装置に対して、上記コンテンツの復号化鍵を送信する管理サーバ装置とを有するコピー管理システム。

【請求項2】 請求項1記載のコピー管理システムであって、

上記管理サーバ装置は、一つの媒体識別情報に対して1回のみ復号化鍵の送信を行うことを特徴とするコピー管理システム。

【請求項3】 請求項1又は請求項2記載のコピー管理システムであって、

上記端末装置は、上記端末装置の識別情報、上記コンテンツのコピーを行うコピー手段に固有に付された識別情報、及び外付けの半導体メモリに固有に付された識別番号のうち、いずれか1つ或いは複数を組み合わせ、上記デバイス識別情報として送信することを特徴とするコピー管理システム。

【請求項4】 請求項1から請求項3のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、上記デバイス識別情報で上記復号化鍵を暗号化して送信し、

上記端末装置は、自己のデバイス識別情報で、上記暗号化された復号化鍵を復号化して用いることを特徴とするコピー管理システム。

【請求項5】 請求項1から請求項4のうち、いずれか一項記載のコピー管理システムであって、

上記端末装置は、上記コンテンツの復号化後に、上記復号化鍵を削除することを特徴とするコピー管理システム。

【請求項6】 請求項1から請求項5のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信し、

上記端末装置は、上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーし、上記再暗号化鍵を記憶手段に記憶し、上記記憶手段に記憶した再暗号化鍵を用いて、上記コピーされたコンテンツを復号化して再生することを特徴とするコピー管理システム。

【請求項7】 請求項1から請求項6のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、各ユーザのデバイス識別情報に関連付けして上記復号化鍵を送信済みの媒体識別情報をデータベースに記憶することで上記復号化鍵の配信管理を行い、修理或いは交換によりユーザのデバイス識別情報が変更された場合、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えることを特徴とするコピー管理システム。

【請求項8】 請求項1から請求項7のうち、いずれか一項記載のコピー管理システムであって、

上記管理サーバ装置は、復号化鍵の送信を行った端末装置を有するユーザに対して所定の課金処理を行うことを特徴とするコピー管理システム。

【請求項9】 請求項1から請求項8のうち、いずれか一項記載のコピー管理システムであって、

上記ユーザの端末装置と上記管理サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記復号化鍵をユーザの端末装置に送信した際に、ユーザに対する課金処理を行う仲介サーバ装置を有することを特徴とするコピー管理システム。

【請求項10】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、

ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、

少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、

上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、

上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、

上記復号化処理したコンテンツをコピーするステップとを有するクライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項11】 請求項10記載の記憶媒体であって、上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、

上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理することを特徴とする記憶媒体。

【請求項12】 請求項10又は請求項11記載の記憶媒体であって、

上記コンテンツのコピー後に、上記復号化鍵を削除するステップを有することを特徴とする記憶媒体。

【請求項13】 請求項10から請求項12のうち、い

いずれか一項記載の記憶媒体であって、  
上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、  
上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、  
上記再暗号化鍵を記憶手段に記憶するステップと、  
コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップとを有することを特徴とする記憶媒体。

【請求項 14】 請求項 10 から請求項 13 のうち、いずれか一項記載の記憶媒体であって、  
上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信することを特徴とする記憶媒体。

【請求項 15】 ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、  
各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップとを有する管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 16】 請求項 15 記載の記憶媒体であって、  
上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有することを特徴とする記憶媒体。

【請求項 17】 請求項 15 又は請求項 16 記載の記憶媒体であって、  
上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信することを特徴とする記憶媒体。

【請求項 18】 請求項 15 から請求項 17 のうち、いずれか一項記載の記憶媒体であって、  
上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信することを特徴とする記憶媒体。

【請求項 19】 請求項 15 から請求項 18 のうち、いずれか一項記載の記憶媒体であって、  
修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有することを特徴とする記憶媒体。

【請求項 20】 請求項 15 から請求項 19 のうち、いずれか一項記載の記憶媒体であって、  
上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有することを特徴とする記憶媒体。

【請求項 21】 請求項 15 から請求項 20 のうち、いずれか一項記載の記憶媒体であって、  
上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする記憶媒体。

【請求項 22】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、  
ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出すステップと、  
少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信するステップと、  
上記媒体識別情報及びデバイス識別情報を送信することで、上記管理者側のサーバ装置から返信される復号化鍵を受信するステップと、  
上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理するステップと、  
上記復号化処理したコンテンツをコピーするステップとを有するクライアント端末装置の情報処理プログラム。

【請求項 23】 請求項 22 記載の情報処理プログラムであって、  
上記復号化鍵を受信するステップは、ユーザのデバイスのデバイス識別情報で暗号化されて送信される復号化鍵を受信し、  
上記コンテンツを復号化処理するステップは、自己のデバイスのデバイス識別情報で、上記暗号化されている復号化鍵を復号化処理し、この復号化処理した復号化鍵を用いて上記記憶媒体に記憶されているコンテンツを復号化処理することを特徴とする情報処理プログラム。

【請求項 24】 請求項 22 又は請求項 23 記載の情報処理プログラムであって、  
上記コンテンツのコピー後に、上記復号化鍵を削除する

ステップを有することを特徴とする情報処理プログラム。

【請求項25】 請求項22から請求項24のうち、いずれか一項記載の情報処理プログラムであって、上記管理サーバ装置から送信される、上記コピーするコンテンツを再暗号化するための再暗号化鍵を受信するステップと、上記復号化鍵で復号化したコンテンツを、上記再暗号化鍵で再暗号化してコピーするステップと、上記再暗号化鍵を記憶手段に記憶するステップと、コンテンツを再生する際に、上記記憶手段に記憶されている再暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップとを有することを特徴とする情報処理プログラム。

【請求項26】 請求項22から請求項25のうち、いずれか一項記載の情報処理プログラムであって、上記媒体識別情報及びデバイス識別情報を送信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を送信することを特徴とする情報処理プログラム。

【請求項27】 ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出するステップと、上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するステップとを有する管理サーバ装置の情報処理プログラム。

【請求項28】 請求項27記載の情報処理プログラムであって、上記復号化鍵の送信を行った媒体識別情報を、該送信を行ったユーザのデバイスのデバイス識別番号に関連付けて上記データベースに登録するステップを有することを特徴とする情報処理プログラム。

【請求項29】 請求項27又は請求項28記載の情報処理プログラムであって、上記復号化鍵を送信するステップは、ユーザのデバイスのデバイス識別情報で、上記復号化鍵を暗号化して送信することを特徴とする情報処理プログラム。

【請求項30】 請求項27から請求項29のうち、い

ずれか一項記載の情報処理プログラムであって、上記復号化鍵を送信するステップは、上記コピーするコンテンツを再暗号化するための再暗号化鍵を送信することを特徴とする情報処理プログラム。

【請求項31】 請求項27から請求項30のうち、いずれか一項記載の情報処理プログラムであって、修理或いは交換によりユーザのデバイスに対して新たなデバイス識別情報が付与された際に、上記データベースに登録されている古いデバイス識別情報を新たなデバイス識別情報に書き換えるステップを有することを特徴とする情報処理プログラム。

【請求項32】 請求項27から請求項31のうち、いずれか一項記載の情報処理プログラムであって、上記復号化鍵の送信を行ったユーザに対して課金を行うステップを有することを特徴とする情報処理プログラム。

【請求項33】 請求項27から請求項32のうち、いずれか一項記載の記載の情報処理プログラムであって、上記媒体識別情報及びデバイス識別情報受信するステップでは、該デバイス識別情報として、ユーザが使用する端末装置に対して固有に付されている識別情報、上記コンテンツがコピーされる二次記憶装置に対して固有に付されている識別情報、或いは上記端末装置に対して外付けされるメモリに対して固有に付されている識別情報のうち、いずれかの識別情報或いは複数の識別情報を受信することを特徴とする情報処理プログラム。

【請求項34】 固有のデバイス識別番号が付されたユーザのデバイスで、固有の媒体識別情報が付された記憶媒体に暗号化鍵で暗号化されて記憶されているコンテンツのコピーを行う際に、上記デバイスから上記デバイス識別情報及び上記媒体識別情報を管理サーバ装置に送信し、コンテンツのコピーが行われた記憶媒体の媒体識別情報が、各ユーザのデバイスのデバイス識別情報に関連付けされた状態で登録されるデータベースに、上記ユーザのデバイスから送信された媒体識別情報が登録されているか否かを上記管理サーバ装置が検出し、上記データベースに、上記媒体識別情報が未登録であった場合に、上記管理サーバ装置からユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信するコピー管理方法。

【請求項35】 暗号化鍵で暗号化されたコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出し、ユーザが上記コンテンツのコピーを行う際に使用するデバイスに対して固有に付されたデバイス識別情報を読み出し、少なくとも上記読み出した媒体識別情報及びデバイス識別情報を、管理者側のサーバ装置に送信し、上記媒体識別情報及びデバイス識別情報を送信すること

で、上記管理者側のサーバ装置から返信される復号化鍵を受信し、  
上記受信した復号化鍵を用いて、上記記憶媒体に記憶されているコンテンツを復号化処理し、  
上記復号化処理したコンテンツをコピーするクライアント端末装置の情報処理方法。

【請求項 36】 ユーザのデバイスから送信される、該デバイスに対して固有に付されたデバイス識別情報、及び暗号化鍵で暗号化されたコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信し、  
各ユーザのデバイスのデバイス識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースに、上記受信した媒体識別情報が登録されているか否かを検出し、  
上記デバイス識別情報の未登録が検出された際に、ユーザのデバイスに対して、上記コンテンツを復号化するための復号化鍵を送信する管理サーバ装置の情報処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、例えばゲームコンテンツ、映画コンテンツ、音楽コンテンツ、アプリケーションプログラム等のコンピュータプログラムのコピー管理を行うコピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、コピー管理方法、クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法に関する。

【0002】

【従来の技術】 今日において、例えば CD-ROM、DVD-ROM 或いは半導体メモリ等の記憶媒体に記憶されているゲームコンテンツに基づいてビデオゲームを実行するビデオゲーム機が広く普及している。

【0003】 ユーザは、所望のゲームコンテンツが記憶された記憶媒体を購入し、この記憶媒体をビデオゲーム機で再生してビデオゲームを行う。大抵の場合、ユーザは、徐々に新しいビデオゲームを買い揃えていく。このため、月日と共にユーザの手元には各ゲームコンテンツが記憶された記憶媒体が蓄積されていくこととなる。

【0004】 しかし、ビデオゲーム機には、記憶媒体の再生機構が 1 基のみ設けられている場合が多い。このため、異なるビデオゲームを行う場合には、ビデオゲーム機に現在装着されている記憶媒体を取り出し、これから行おうとするゲームコンテンツが記憶された記憶媒体を新たに装着し直すという、大変面倒な作業を必要としていた。

【0005】

【発明が解決しようとする課題】 本件出願人は、例えば数十 G（ギガ）オーダーの大容量のハードディスクドライブ（HDD）を内蔵或いは外付け可能としたビデオゲーム機を開示している。

【0006】 このビデオゲーム機の場合、各記憶媒体に記憶されているゲームコンテンツをそれぞれ HDD にコピーし、この HDD から所望のゲームコンテンツを再生して利用することができる。この HDD を用いることにより、ビデオゲーム機の再生機構に記憶媒体を着脱する手間を省略することができる。

【0007】 ここで、ゲームコンテンツ等のコンピュータプログラムは、そのコンピュータプログラムが記憶されたソフトウェアを購入する等して正当に入手したユーザのみが使用可能なはずである。

【0008】 しかし、記憶媒体に記憶されたコンピュータプログラムを二次記憶媒体にコピー可能とした場合、一つの記憶媒体に記憶されているコンピュータプログラムを、複数のユーザがそれぞれ二次記憶媒体にコピーして使用する不正コピーが懸念される。

【0009】 本発明は、上述の課題に鑑みてなされたものであり、正当なユーザに対してのみ、コンピュータプログラムのコピーを可能とするコピー管理を行うことで、コンテンツの不正使用の防止等を図ったコピー管理システム、クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体、クライアント端末装置の情報処理プログラム、管理サーバ装置の情報処理プログラム、コピー管理方法、クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法の提供を目的とする。

【0010】

【課題を解決するための手段】 本発明は、暗号化鍵で暗号化したコンテンツを記憶させた記憶媒体に対して固有の識別番号を付してユーザに配布する。ユーザがコンテンツのコピーを行う際に使用するデバイスにも識別番号が付されている。

【0011】 上記デバイスは、コンテンツのコピーを行う際に、上記記憶媒体の識別番号、及びデバイスの識別番号を管理サーバ装置に送信する。管理サーバ装置は、各ユーザが使用するデバイスの識別番号が登録されたデータベースを有している。管理サーバ装置は、データベースに登録されているデバイスの識別番号と、ユーザのデバイスから送信されたデバイスの識別番号とを照合してユーザを特定する。管理サーバ装置は、この照合を行うことでユーザが特定された際に、記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザのデバイスに送信する。

【0012】 ユーザのデバイスは、この管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されて

いるコンテンツを復号化してコンテンツのコピーを行う。

【0013】これにより、記憶媒体の持ち主である正規のユーザにのみ、コンテンツのコピーを許可することができ、コンテンツの不正コピーを防止することができる。

【0014】

【発明の実施の形態】本発明は、コンピュータプログラムのコピー管理を行うコピー管理システムに適用することができる。

【0015】コンピュータプログラムとしては、例えばゲームコンテンツ、音楽コンテンツ、映画コンテンツ、アプリケーションプログラム等がある。また、コンピュータプログラムが記憶された記憶媒体としては、DVD-ROM、CD-ROM等の光ディスクの他、半導体メモリがある。また、コンピュータプログラムのコピー先となる二次記憶媒体としては、ハードディスク(HD)、DVD-RAMや光磁気ディスク(MO)等がある。

【0016】以下、上記ゲームコンテンツ、音楽コンテンツ、映画コンテンツ、アプリケーションプログラム等を総称して、単に「コンテンツ」ということとする。

【0017】[コピー管理システムの全体構成] まず、図1に本発明の第1の実施の形態となるコピー管理システムの全体構成を示す。この図1に示すように、この第1の実施の形態のコピー管理システムは、光ディスクに記憶されているコンテンツの再生機能(実行機能)、及びネットワークを介した通信機能を備えたクライアント端末装置1を有している。

【0018】このクライアント端末装置1には、光ディスクに記憶されたコンテンツをコピーするためのハードディスクドライブ2(HDD)が接続されている。

【0019】また、このクライアント端末装置1には、インターネット5などのネットワークとの接続を図るための通信モデム6が接続されている。

【0020】なお、通信モデム6は、この図1に示すようにクライアント端末装置1に対して外付けのかたちで設けてもよい。また、通信モデム6は、クライアント端末装置1に内蔵のかたちで設けてもよい。

【0021】また、コピー管理システムは、ユーザエントリ情報が記憶されたデータベース3を備えたシステムサーバ装置4を有している。

【0022】このシステムサーバ装置4と上記クライアント端末装置1とが、例えばインターネット5等のネットワークを介して相互に接続されることでこの第1の実施の形態のコピー管理システムが構成されている。

【0023】[クライアント端末装置の構成] 図2に、クライアント端末装置1の外観の斜視図を示す。この図2示すように、クライアント端末装置1の前面側には、コントローラ接続部7A、7Bと、メモ리카ード装着部

8A、8Bが設けられている。

【0024】また、このクライアント端末装置1の前面側には、USB対応機器(USB:Universal Serial Bus)が接続される2つのUSB接続端子9と、例えば最大400Mbpsのデータ転送速度に対応可能なIEEE1394接続端子10とが設けられている。

【0025】また、このクライアント端末装置1の前面側には、光ディスクが装着されるトレイ型のディスク装着部11が設けられている。

【0026】また、このクライアント端末装置1の前面側には、コンテンツの実行動作や再生動作をリセットするためのリセットボタン12と、光ディスク装着部11のトレイの出し入れを操作するためのトレイ操作ボタン13とが設けられている。

【0027】クライアント端末装置1の背面側には、電源スイッチ、音声映像出力端子(AVマルチ出力端子)、PCカードスロット、光デジタル出力端子、AC電源入力端子等が設けられている。

【0028】AVマルチ出力端子は、AVケーブル17を介してモニタ用のテレビジョン受像機18に接続される。クライアント端末装置1から出力される映像信号や音声信号は、このAVマルチ出力端子及びAVケーブル17を介してモニタ用のテレビジョン受像機18に供給される。これにより、上記コンテンツの映像がテレビジョン受像機18に表示される。また、上記コンテンツの音声はテレビジョン受像機のスピーカ装置を介して発音される。

【0029】コントローラ接続部7A、7Bには、コントローラケーブル15を介してそれぞれコントローラ14が接続される。

【0030】メモ리카ード装着部8A、8Bには、ゲームデータのセーブ(記憶)及び読み出しを行うセーブ用のメモ리카ード等が装着される。

【0031】[ハードディスクドライブの構成] 次に、図2において、クライアント端末装置1の上面部に載置されている筐体がハードディスクドライブ2(以下、HDD2という)である。このHDD2は、内部に例えば40GB等の大容量のハードディスクが設けられている。このHDD2には、十数枚分のDVD-ROMに記憶されたゲームコンテンツをコピー可能となっている。

【0032】HDD2の前面側には、電源投入時に点灯駆動される電源ランプ20と、ハードディスクへの書き込みに連動して点灯駆動される書き込み表示ランプ21とが設けられている。HDD2の背面側には、少なくとも電源スイッチ及びデータ入出力端子が設けられている。

【0033】HDD2をクライアント端末装置1に接続する場合、クライアント端末装置1の背面側に設けられた上記PCカードスロットにPCカードを挿入する。この状態で、PCカードに接続ケーブルの一端を接続す



る。接続ケーブルの他端は、HDD2のデータ入出力端子に接続する。これにより、クライアント端末装置1とHDD2とが、電氣的に相互に接続される。

【0034】なお、この例においては、HDD2はクライアント端末装置1とは別体で、クライアント端末装置1に対して外付けすることとした。しかし、このHDD2を、クライアント端末装置1に内蔵するかたちで設けてもよい。

【0035】また、クライアント端末装置1とHDD2とをPCカードと接続ケーブルを介して接続することとした。しかし、HDD2の背面側（或いは前面側でもよい。）にUSB接続端子やIEEE1394接続端子等の接続端子を設け、この接続端子を介してHDD2をクライアント端末装置1に接続するようにしてもよい。

【0036】〔クライアント端末装置の電氣的構成〕次に、図3はクライアント端末装置1のブロック図である。この図3に示すように、クライアント端末装置1は、CPU30と、グラフィックプロセッサ31（GPU）と、IOPロセッサ32（IOP）を有している。

【0037】また、クライアント端末装置1は、CD-ROMやDVD-ROM等の光ディスクの再生制御を行う光ディスク制御部33と、サウンドプロセッサユニット34（SPU）とを有している。

【0038】また、クライアント端末装置1は、CPU30やIOP32が実行するオペレーティングシステムプログラムが格納されたMASK-ROM35と、CPU30のワークエリアや光ディスクから読み出されたデータを一時的に格納するバッファとして機能するRAM36とを有している。

【0039】また、クライアント端末装置1は、光ディスク制御部33のRFアンプ37を介して供給される光ディスクからの再生出力に対して、例えば誤り訂正処理（CIRC処理）等を施して出力するCD/DVDDSP38を有している。

【0040】また、クライアント端末装置1は、光ディスク制御部33のスピンドルモータの回転制御、光ピックアップのフォーカス／トラッキング制御、ディスクトレイのローディング制御等を行うドライバ39及びメカコントローラ40を有している。

【0041】また、クライアント端末装置1は、上記PCカードが接続されるカード型コネクタ41を有している。

【0042】これらの各部は、主にバスライン42、43等を介してそれぞれ相互に接続されている。

【0043】なお、DVD-ROMに記憶された映画コンテンツの再生は、メモリカードに記憶されたDVDドライバソフトウェアに基づいて行われる。或いは、映画コンテンツの再生は、クライアント端末装置1内に内蔵された半導体メモリ44（DVD Player ROM）に焼き付けられたDVDドライバソフトウェアに基づいて行

われる。

【0044】MASK-ROM35には、オペレーティングシステムプログラムが記憶されている。CPU30は、このMASK-ROM35に記憶されているオペレーティングシステムプログラムに基づいて、クライアント端末装置1全体の動作を制御する。

【0045】また、MASK-ROM35には、コントローラ接続部7A、7Bと、メモリカード装着部8A、8B、及びカード型コネクタ41に接続されるコントローラ14、メモリカード16及びHDD2等のハードウェア識別番号（ハードウェアID）も記憶されている。IOP32は、このMASK-ROM35に記憶されているハードウェアIDに基づいて、コントローラ14、メモリカード16及びHDD2等のハードウェアと通信を行い、各接続端子7A、7B、8A、8B及びカード型コネクタ41等に接続されたハードウェアを特定して認識する。

【0046】なお、ハードウェアIDは、クライアント端末装置1全体で一つのID、メモリカード16全体で一つのID、及びHDD2全体で一つのID等のように、いわば各ハードウェアに対して総称的に付されたIDを意味している。

【0047】これに対して、後述するクライアントID、MC-ID及びHDD-IDは、各クライアント端末装置1毎、各メモリカード16毎、及び各HDD2毎にそれぞれ付された各ハードウェア固有のIDとなっている。

【0048】GPU31は、CPU30からの描画指示に従って描画を行い、描画された画像を図示しないフレームバッファに格納する。また、GPU31は、座標変換等の処理を行うジオメトリトランスファエンジンとしての機能を有している。

【0049】このGPU31は、例えば光ディスクに記録されているゲームコンテンツがいわゆる3Dグラフィックを利用する場合に、三角形のポリゴンの集合で仮想的な3次元オブジェクトを構成する。そして、GPU31は、この3次元オブジェクトを仮想的なカメラ装置で撮影することで得られる画像を生成するための諸計算を行う。すなわち、GPU31は、レンダリングを行う場合における透視変換処理（3次元オブジェクトを構成する各ポリゴンの頂点を仮想的なカメラスクリーン上に投影した場合における座標値の計算）等を行う。

【0050】また、GPU31は、CPU30からの描画指示に従って、必要に応じてジオメトリトランスファエンジンを利用しながら、フレームバッファに対して描画を行う。そして、この描画した画像に対応するビデオ信号（visual out）を出力する。

【0051】一方、SPU34は、適応予測符号化された音声データを再生するADPCM復号機能と、サウンドバッファに記憶されている波形データを再生すること

で、効果音等の音声信号を再生して出力（audio out）する再生機能と、サウンドバッファに記憶されている波形データを変調させて再生する変調機能等を備えている。このSPU34は、いわゆるサンプリング音源として動作する。SPU34は、CPU30からの指示により、サウンドバッファに記憶されている波形データに基づき楽音、効果音等の音声信号を発生する。

【0052】このようなクライアント端末装置1は、電源が投入されると、CPU30及びIOP32が、MASK-ROM35からCPU30用のオペレーティングシステムプログラム及びIOP32用のオペレーティングシステムプログラムをそれぞれ読み出す。

【0053】CPU30は、CPU30用のオペレーティングシステムプログラムによりクライアント端末装置1の各部を統括的に制御する。IOP32は、IOP32用のオペレーティングシステムプログラムによりコントローラ14、メモリカード16、及びHDD2等との間のデータの入出力を制御する。

【0054】CPU30は、CPU30用のオペレーティングシステムプログラムに基づいて、動作確認等の初期化処理を行った後、光ディスク制御部33を制御し、光ディスクに記録されているコンテンツを再生制御する。

【0055】再生したコンテンツがビデオゲームのゲームコンテンツである場合、CPU30は、IOP32を介してコントローラ14から受け付けたプレーヤからの指示（コマンド）に従って、GPU31やSPU34を制御し、ゲームコンテンツの画像の表示や効果音、楽音等の発声を制御する。

【0056】再生したコンテンツが映画コンテンツの場合、CPU30は、IOP32を介してコントローラ14から受け付けたプレーヤからの指示に従って、GPU31やSPU34を制御し、映画コンテンツの映像の表示や音声の発声等を制御する。

【0057】〔コピー管理動作〕このようなコピー管理システムは、光ディスクに記憶されているコンテンツがHDD2にコピーされる際に、以下のように管理する。

【0058】〔インストーラのインストール〕まず、このコピー管理システムは、光ディスクに記憶されているコンテンツをHDD2にコピーする際に、クライアント端末装置1でコピー制御用のアプリケーションプログラム（インストーラ）を実行する必要がある。この例の場合、インストーラは、コンテンツと共に光ディスクに記憶されている。クライアント端末装置1は、コンテンツのコピーを行う前にインストーラのインストールを行う。

【0059】インストーラのインストールを行う場合、ユーザは、インストーラが記憶されている光ディスクをクライアント端末装置1に装着する。クライアント端末装置1のCPU30は、この光ディスクが装着されると自動的に（オートラン）、或いはユーザのコントローラ

14の操作に従って光ディスクに記憶されているインストーラを読み出し、これをメモリカード16或いはRAM36に記憶制御する。

【0060】このメモリカード16或いはRAM36に記憶されたインストーラは、ユーザが光ディスクに記憶されているコンテンツのコピーを指定した際に、CPU30により実行される。CPU30は、このインストーラを実行することで、コンテンツのコピー制御を行う。

【0061】なお、インストーラは、システム業者側でインストーラのみ記憶された光ディスクを製造し、これをユーザに配布するようにしてもよい。或いは、システム業者側でインストーラが記憶されたメモリカードを製造し、これをユーザに配布するようにしてもよい。この場合、インストーラのインストール作業を省略可能とすることができる。

【0062】或いは、インストーラが記憶されたROMをクライアント端末装置1内に設けてもよい。この場合でも、インストーラのインストール作業を省略可能とすることができる。

【0063】〔コンテンツの暗号化〕光ディスクに記憶されたコンテンツには、図4に示すように各コンテンツ毎に異なる対称鍵（コンテンツキー：Content Key）を用いて暗号化処理が施されている。また、光ディスクには、このように暗号化処理されたコンテンツの他、各光ディスク毎に固有となる「Media unique ID（メディアユニークID：MID）」が記憶されている。

【0064】〔ユーザ登録〕次に、この第1の実施の形態のコピー管理システムにおいては、光ディスクからHDD2にコンテンツのコピーを行う場合、各メモリカード16に固有に付された「メモリカードID（MC-ID）」を用いてシステムサーバ装置4にユーザ登録を行う。このユーザ登録が行われない場合には、コンテンツのコピーは許可されない。

【0065】図5は、ユーザがシステムサーバ装置4に対してユーザ登録を行うまでの流れを示すフローチャートである。図6は、このユーザ登録によりクライアント端末装置1とシステムサーバ装置4との間で送受信される情報を示す当該コピー管理システムの模式図である。

【0066】この図5及び図6を用いてユーザ登録動作を説明する。図5のフローチャートは、ユーザがクライアント端末装置1のメイン電源を投入することでスタートとなる。

【0067】ステップS1では、ユーザがインターネット5を介して自分のクライアント端末装置1をシステムサーバ装置4に接続する。

【0068】具体的には、このクライアント端末装置1には、図1に示したようにインターネット接続用の通信モデム6が接続（或いは内蔵）されている。ユーザによりインターネット接続が指定されると、図3に示すCP

U30は、所定のWWWブラウザに基づいて動作し、この通信モデム6を介して当該クライアント端末装置1とシステムサーバ装置4との間の通信回線の確立を図る。これにより、このユーザ登録の行程がステップS2に進む。

【0069】ステップS2では、CPU30が、クライアント端末装置1に装着されたメモリカードの識別番号(MC-ID)、クライアント端末装置1毎に付された固有の識別番号(クライアントID)及びHDD2毎に付された固有の識別番号(HDD-ID)をシステムサーバ装置4に送信制御する。

【0070】具体的には、システムサーバ装置4とクライアント端末装置1との通信回線が確立されると、CPU30は、クライアント端末装置1、HDD2及びメモリカード16とそれぞれ通信を行う。CPU30は、この通信により、クライアント端末装置1に固有に付された識別番号(クライアントID)、HDD2に固有に付された識別番号(HDD-ID)、及びクライアント端末装置1に装着されたメモリカード16に固有に付された識別番号(MC-ID)をそれぞれ取得する。

【0071】CPU30は、これらの識別番号を、図6に示すようにシステムサーバ装置4側に送信する。これにより、このユーザ登録の行程がステップS3に進む。

【0072】なお、クライアント端末装置1とシステムサーバ装置4との間においては、例えばSSL(Secure Sockets Layer)等の通信プロトコルに基づいて情報が暗号化されて送受信されるようになっており、通信の安全性が確保されている。

【0073】また、この例においては、CPU30は、各デバイスと通信を行うことで、クライアントID、HDD-ID及びMC-IDを取得してシステムサーバ装置4側に送信することとした。しかし、クライアント端末装置1、HDD2及びメモリカード16には、クライアントID、HDD-ID及びMC-IDがそれぞれ各筐体にユーザが視認可能なかたちで貼り付けられている。このため、ユーザが、このクライアントID、HDD-ID及びMC-IDを見て、コントローラ14を操作して手動で各IDの入力を行い、システムサーバ装置4側に送信するようにしてもよい。

【0074】次に、ステップS3では、システムサーバ装置4が、このユーザから送信されたメモリカードの識別番号(MC-ID)が有効なIDであるか否かを判別する。このユーザ登録行程は、このステップS3において、システムサーバ装置4が、ユーザから送信されたMC-IDが有効なIDであると判別した場合にステップS4に進み、ユーザから送信されたMC-IDが無効なIDであると判別した場合にステップS7に進む。

【0075】具体的には、システムサーバ装置4は、全てのクライアント端末装置1のクライアントID、全てのHDD2のHDD-ID、及び全てのメモリカード1

6のMC-IDを記憶したデータベース3を有している。

【0076】システムサーバ装置4は、ユーザからクライアント端末装置1、HDD2及びメモリカード16の各固有のIDが送信されると、まず、ユーザから送信されたメモリカード16の固有のIDであるMC-IDと、データベース3に登録されている各MC-IDとを照合し、ユーザから送信されたメモリカード16のMC-IDと同じMC-IDがデータベース3に登録されているか否かを判別する。

【0077】すなわち、システムサーバ装置4は、ユーザから送信されたメモリカード16のMC-IDは、データベース3に正規に登録されているMC-IDと同じであるか否かを判別する。

【0078】ユーザから送信されたメモリカード16のMC-IDが、データベース3に正規に登録されているいずれのMC-IDとも一致しなかった場合には、システムサーバ装置4は、このユーザ登録のアクセスを、不正なユーザ登録のアクセスと判断する。この場合、システムサーバ装置4は、ステップS7において、例えば「このメモリカードではユーザ登録を行うことはできません。」等のユーザ登録を拒否するメッセージをクライアント端末装置1側に返信する(無効通知)。これにより、ユーザ登録が中断されたかたちで、このユーザ登録行程が終了することとなる。

【0079】一方、ユーザから送信されたメモリカード16のMC-IDが、データベース3に正規に登録されているいずれかのMC-IDと一致した場合、システムサーバ装置4は、ステップS4において、現在、システムサーバ装置4にアクセスしているユーザの固有のIDであるユーザID(User ID)を、例えば乱数等を用いて形成する。

【0080】そして、システムサーバ装置4は、図6に示すようにそのユーザのクライアントID、HDD-ID及びMC-IDと共に、上記ユーザの固有のIDであるユーザID(User ID)、及び後に説明するMC-Keyを一纏めにし、これを「ユーザエントリ情報」としてシステムサーバ装置4のデータベース3に登録する。

【0081】このように、当該実施の形態のコピー管理システムは、各ユーザが所有するクライアント端末装置1、HDD2及びメモリカード16の3つのIDの組み合わせで各ユーザを特定してデータベース3に登録する。

【0082】クライアント端末装置1、HDD2及びメモリカード16の3つのIDが、異なるユーザ間で全て一致するということは有り得ないため、この3つのIDに基づいてユーザ登録を行うことにより、ユーザを確実に特定してユーザ登録を行うことができる。これにより、後述する光ディスクに記録されたコンテンツの不正

コピーを、より強力に防止することができる。

【0083】なお、ユーザ登録の際に、「MC-IDのみ」、「クライアントIDのみ」、「HDD-IDのみ」、「MC-IDとクライアントID」、「MC-IDとHDD-ID」、或いは「クライアントIDとHDD-ID」をシステムサーバ装置4側に送信してユーザ登録を行うようにしてもよい。これらの場合でも、各IDはそれぞれ固有のIDであるため、異なるユーザ間で重複することはなく、ユーザを略々確実に特定してユーザ登録を行うことができる。

【0084】次に、ユーザ登録の行程がステップS5に進むと、システムサーバ装置4は、ユーザ登録が正規に完了した証として、上記ステップS4で形成したユーザエントリ情報のうち、ユーザID (User ID) をMC-Keyで暗号化し、これをクライアント端末装置1側に返信する。

【0085】〔MC-Key〕ここで、上記「MC-Key」は、クライアント端末装置1とシステムサーバ装置4との間で送受信する情報を暗号化するための鍵情報である。このMC-Keyは、MC-IDと共にメモリカード16内に予め記憶されている。

【0086】MC-IDは、ユーザが視認可能のようにメモリカード16の筐体に張り付けられているのであるが、このMC-Keyはユーザが視認できないようにメモリカード16内に記憶されている。また、このMC-Keyは、ユーザがメモリカード16内に記憶されている情報を再生した場合でも、表示や出力が行われることのない秘密性の高い情報となっている。このため、このMC-Keyは、ユーザレベルでは、認識することはできないようになっている。

【0087】また、システムサーバ装置4のデータベース3には、全てのメモリカード16のMC-IDと共に、各メモリカード16に記憶されたMC-Keyが記憶されている。システムサーバ装置4は、MC-Keyが必要となったときに、このデータベース3からMC-Keyを読み出して参照する。このため、クライアント端末装置1からシステムサーバ装置4に対してMC-Keyが送信されることはない。

【0088】このように、MC-Keyは、ユーザレベルでは認識することができず、また、クライアント端末装置1とシステムサーバ装置4との間で送受信されることの無い、秘密性の高い情報となっている。

【0089】クライアント端末装置1とシステムサーバ装置4との間におけるMC-Keyの送受信を不要とすることで、MC-Keyが第三者に傍受される不都合を防止することができる。

【0090】システムサーバ装置4は、ユーザID (User ID) を返信する際、予めデータベース3に記憶されているMC-Keyの中から、現在アクセスされているユーザのメモリカード16に対応するMC-Key

yを選択する。そして、この選択したMC-Keyを用いてユーザID (User ID) を暗号化してクライアント端末装置1に返信する。

【0091】このMC-Keyは、上記ユーザID (User ID)、メディアユニークID (media unique ID (MID))、コンテンツキー (Content-Key)、及びContent-Gen-Keyをそれぞれ復号化する際に用いられる。

【0092】MIDは、各光ディスク毎に固有に付されているIDである。コンテンツキーは、光ディスクに記録されたコンテンツを暗号化処理する際に用いられた暗号鍵である。Content-Gen-Keyは、HDD2にコピーされるコンテンツに対して再暗号化処理を施す際に用いられる暗号鍵である。

【0093】クライアント端末装置1は、光ディスクから再生したコンテンツを、上記コンテンツキーを用いて復号化する。そして、クライアント端末装置1は、この復号化したコンテンツを、上記Content-Gen-Keyを用いて再暗号化処理してHDD2にコピーするようになっている。詳しくは後述する。

【0094】次に、ユーザ登録行程がステップS6に進むと、クライアント端末装置1が、システムサーバ装置4側から返信されたユーザID (User ID) をメモリカード16に記憶制御する。これにより、この図5のフローチャートに示すユーザ登録の全行程が終了する。そして、この時点において、メモリカード16には、図6に示すように予め記憶されているMC-ID及びMC-Keyと共に、MC-Keyで暗号化されたユーザID (User ID) が記憶されることとなる。

【0095】〔メディアユニークIDの登録とコンテンツキーの取得〕次に、光ディスクに記録されているコンテンツを何回でもHDD2にコピー可能とすると、MC-ID、MC-Key及びユーザID (User ID) が記録されたメモリカード16を他のユーザに貸与するだけで、この他のユーザも光ディスクに記録されているコンテンツをこの他のユーザのHDDに不正にコピーすることが可能となり好ましいことではない。

【0096】このコピー管理システムの場合、コンテンツをHDD2にコピーする際、ユーザがクライアント端末装置1を介して各光ディスク毎に付された固有のメディアユニークID (media unique ID (MID)) をシステムサーバ装置4側に送信する。システムサーバ装置4は、ユーザから送信されたメディアユニークIDを登録すると共に、暗号化されたコンテンツを復号化するためのコンテンツキーをユーザに送信する。クライアント端末装置1は、光ディスクに記録されているコンテンツを、コンテンツキーを用いて復号化してHDD2にコピーする。このため、このコンテンツキーを受信するということは、システムサーバ装置4からクライアント端末装置1に対して、コンテンツのコピー

が許諾されたことを意味する。

【0097】システムサーバ装置4は、クライアント端末装置1から受信したメディアユニークIDに対して、過去にコンテンツキーの送信が行われていないことを確認したうえで、コンテンツキーの送信を行う。これにより、同じメディアユニークIDに対するコンテンツキーの送信を、1回のみに制限することができる。

【0098】例えば、あるユーザが自分で購入した光ディスクに記憶されているコンテンツを、自分のHDD2にコピーした後に、この光ディスクを他のユーザに貸与したとする。他のユーザは、HDD2にコンテンツをコピーする際に、貸与された光ディスクのメディアユニークIDをシステムサーバ装置4に送信する。

【0099】しかし、システムサーバ装置4側には、その光ディスクのメディアユニークIDに対して、コンテンツキーの送信が行われたことを示す履歴が残っている。この場合、システムサーバ装置4は、他のユーザに対してコンテンツキーの配信は行わない。コンテンツキーを入手することができない他のユーザは、コンテンツをHDD2にコピーすることはできない。このコピー管理システムは、このようにしてコンテンツの不正コピーを防止している。

【0100】図7のフローチャートに、メディアユニークID(MID)の登録とユーザがコンテンツキーを取得するまでの流れを示す。また、図8に、メディアユニークIDの登録の際、及びコンテンツキーの取得の際に、クライアント端末装置1とシステムサーバ装置4との間で送受信される各情報を示す。

【0101】この図7及び図8を用いてメディアユニークID(MID)の登録とコンテンツキーの取得動作を説明する。この図7のフローチャートに示すメディアユニークID(MID)の登録とコンテンツキーの取得行程(登録取得行程)は、ユーザが前述のユーザ登録を正規に終了させていることを前提として実行される。

【0102】まず、ステップS11では、クライアント端末装置1が、システムサーバ装置4との間の通信回線の確立を図る。これにより、この登録取得行程がステップS12に進む。

【0103】なお、この例においては、前述のユーザ登録終了後に、クライアント端末装置1とシステムサーバ装置4との間で確立された通信回線を一旦切断し、この登録取得行程の実行時に、再度、クライアント端末装置1とシステムサーバ装置4との間の通信回線を確立する説明となっている。

【0104】しかし、前述のユーザ登録に続けて、クライアント端末装置1とシステムサーバ装置4との間で確立された通信回線を切断することなく、この登録取得行程を実行するようにしてもよい。この場合、この登録取得行程は、ステップS11をスキップして、スタートからステップS12に進むこととなる。

【0105】次にステップS12では、クライアント端末装置1が、前述のように取得したユーザID(User ID)及びMC-IDをシステムサーバ装置4に送信する。また、クライアント端末装置1は、このユーザID及びMC-IDと共に、これからHDD2にコピーするコンテンツが記憶された光ディスクに対して固有に付されているメディアユニークID(MID)をシステムサーバ装置4側に送信する。

【0106】具体的には、CPU30は、メモ리카ード16と通信を行い、図8に示すようにMC-IDをシステムサーバ装置4側に送信する。また、CPU30は、前述のようにMC-Keyで暗号化されたユーザIDをメモ리카ード16から読み出してシステムサーバ装置4側に送信する。また、CPU30は、光ディスク制御部33を制御して光ディスクから再生したメディアユニークID(MID)をMC-Keyで暗号化し、これをシステムサーバ装置4側に送信する。

【0107】なお、これらの各情報と共に、クライアントID及びHDD-IDをシステムサーバ装置4側に送信するようにしてもよい。クライアントID及びHDD-IDは、上記MC-IDと共にユーザの特定に用いることができる。MC-ID、クライアントID及びHDD-IDの3つのIDを用いてユーザを特定することで、MC-IDのみでユーザの特定を行う場合よりも、より正確にユーザを特定することができる。

【0108】また、クライアント端末装置1とシステムサーバ装置4との間で送受信される情報は、例えばSSL(Secure Sockets Layer)等の通信プロトコルに基づいて暗号化されて送受信される。これにより、クライアント端末装置1とシステムサーバ装置4との間では、安全性の高い通信を行うことができる。

【0109】次に、ステップS13では、システムサーバ装置4が、クライアント端末装置1側から送信されたユーザID(User ID)が有効なIDであるか否かを判別する。このステップS13において、システムサーバ装置4が、ユーザIDは有効であると判別した場合、この登録取得行程がステップS14に進む。これに対して、このステップS13において、システムサーバ装置4が、ユーザIDは無効であると判別した場合、この登録取得行程はステップS17に進む。

【0110】具体的には、システムサーバ装置4は、クライアント端末装置1側から送信されたMC-ID(及びクライアントID、HDD-ID)に基づいてデータベース3を参照し、このMC-IDに対応するMC-Keyを読み出す。そして、システムサーバ装置4は、このMC-Keyに基づいて、MC-Keyで暗号化されて送信されたユーザID(User ID)及びメディアユニークID(MID)をそれぞれ復号化する。

【0111】前述のように、システムサーバ装置4側のデータベース3には、ユーザエン트리情報としてユーザ

ID (User ID), MC-ID, クライアントID及びHDD-ID等が記憶されている。このため、システムサーバ装置4は、MC-ID (クライアントID及びHDD-ID) に基づいてデータベース3内のユーザ情報を検索する。そして、システムサーバ装置4は、このユーザ情報内のユーザID (User ID) と、現在システムサーバ装置4側にアクセスしてきているユーザのユーザID (User ID) とを照合する。システムサーバ装置4は、上記両者が一致した場合には、現在システムサーバ装置4側にアクセスしてきているユーザは正規のユーザであると判断する。これにより、この登録取得行程がステップS14に進む。

【0112】これに対して、システムサーバ装置4は、データベース3のユーザ情報内のユーザID (User ID) と、現在システムサーバ装置4側にアクセスしてきているユーザのユーザID (User ID) とが不一致の場合、そのユーザID (User ID) は無効と判断する。そして、システムサーバ装置4は、ステップS17において、例えば「ユーザIDが無効です。ユーザ登録をして下さい。」等の再度のユーザ登録を促すメッセージをクライアント端末装置1側に返信する(無効通知)。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【0113】次に、ステップS14では、システムサーバ装置4が、現在アクセスしてきているユーザの光ディスクに記録されているコンテンツは、過去にコピーされた履歴があるか否かを判別する。

【0114】具体的には、このコピー管理システムの場合、データベース3に、各光ディスクにそれぞれ付されているメディアユニークID (MID) が全て登録されている。システムサーバ装置4は、コンテンツのコピーが行われた際に、データベース3のメディアユニークID (MID) に対してフラグを立てることで、コピーの履歴を残すようになっている。

【0115】このため、システムサーバ装置4は、メディアユニークID (MID) を復号化すると、そのメディアユニークID (MID) に対してフラグが立っているか否かを検出する。これにより、そのメディアユニークID (MID) を有する光ディスクから過去にコンテンツのコピーが行われたか否かを判別することができる。

【0116】そのメディアユニークID (MID) のフラグが立っていない場合、そのメディアユニークID (MID) が付された光ディスクから過去にコンテンツのコピーは行われていないことを意味する。このため、システムサーバ装置4は、データベース3内におけるそのメディアユニークID (MID) のフラグを立てる。また、システムサーバ装置4は、このフラグを立てたメディアユニークID (MID) を、そのユーザのユーザエントリ情報に登録して、この登録取得行程をステップ

S15に進める。

【0117】これに対して、そのメディアユニークID (MID) のフラグが立っている場合、過去にそのメディアユニークID (MID) が付された光ディスクからコンテンツのコピーが行われていることを意味する。このため、システムサーバ装置4は、ステップS17において、例えば「このメディアからコンテンツのコピーをすることはできません。」等のコンテンツのコピーを拒否するメッセージをクライアント端末装置1側に返信する(無効通知)。これにより、この登録取得行程が中断されたかたちで終了することとなる。

【0118】次にステップS15は、過去に、そのユーザの光ディスクからコンテンツのコピーが行われていない場合に進むステップである。この場合、システムサーバ装置4は、そのユーザのメモリカード16のMC-Keyを用いて、光ディスクに記録されているコンテンツを暗号化したコンテンツキー (Content-Key) の暗号化を行う。そして、この暗号化したコンテンツキーをクライアント端末装置1側に送信する。このコンテンツキーの送信は、システムサーバ装置4側からユーザに対して、光ディスクに記録されているコンテンツのコピーが許可されたことを意味する。

【0119】MC-Keyは、そのユーザが所有するメモリカード16に対して固有に付されている。このため、このコンテンツキーを復号化して使用することができるユーザを、そのMC-Keyが記憶されたメモリカード16を有するユーザのみに限定することができる。従って、上記コンテンツキーを正規のユーザに対してのみ、安全に送信することができる。

【0120】また、システムサーバ装置4は、データベース3に記憶されているユーザエントリ情報に基づいて、そのユーザが使用しているクライアント端末装置1のクライアントID及びHDD2のHDD-IDを読み出す。システムサーバ装置4は、これら各IDを、例えば乱数を用いて形成した「コンテンツジェンキー (Content-Gen-Key)」で暗号化してクライアント端末装置1側に返信する。

【0121】さらに、システムサーバ装置4は、クライアントID及びHDD-IDを暗号化する際に用いたコンテンツジェンキー (Content-Gen-Key) を、上記MC-Keyで暗号化してクライアント端末装置1側に返信する。

【0122】後に説明するが、クライアント端末装置1は、システムサーバ装置4から返信されたクライアントIDと、当該クライアント端末装置1のクライアントIDとを照合する。また、クライアント端末装置1は、システムサーバ装置4から送信されたHDD-IDと、当該クライアント端末装置1に接続されているHDD2のHDD-IDとを照合する。そして、クライアント端末装置1は、上記2つのクライアントIDと、上記2つの

HDD-IDとが、それぞれ一致することを確認してコンテンツのコピーを行うようになっている。

【0123】このため、システムサーバ装置4からユーザのクライアント端末装置1に対して、予め登録されているクライアントID及びHDD-IDを返信することにより、予めデータベース3に登録されているそのユーザのクライアント端末装置1とHDD2の組み合わせでのみ、コンテンツのコピー可能とすることができる。

【0124】さらに、システムサーバ装置4は、クライアントID及びHDD-IDを暗号化したコンテンツジェンキーを、そのユーザが所有するメモリカード16に固有に付されたMC-Keyを用いて暗号化してユーザのクライアント端末装置1に返信する。これにより、コンテンツジェンキーを復号化して使用することができるユーザを、そのMC-Keyが記憶されたメモリカード16を有するユーザのみに限定することができる。従って、上記コンテンツジェンキーを正規のユーザに対してのみ、安全に送信することができる。

【0125】次に、ステップS16では、クライアント端末装置1が、システムサーバ装置4側から返信されたMC-Keyで暗号化されたコンテンツキー(Content-Key)、MC-Keyで暗号化されたコンテンツジェンキー(Content-Gen-Key)、及びコンテンツジェンキー(Content-Gen-Key)で暗号化されたクライアントID及びHDD-IDをそれぞれメモリカード16に記憶制御する。これにより、この図7のフローチャートに示す登録取得行程が終了する。

【0126】このように、このコピー管理システムは、過去にコピー履歴の無いメディアユニークID(MID)を有する光ディスクに記憶されたコンテンツのみコピーの許可を行う。これにより、各光ディスクに記憶されたコンテンツのコピーを1回に制限することができる。このため、過去にコンテンツのコピーが行われた光ディスクを貸与された第三者は、その貸与された光ディスクからコンテンツのコピーを行うことはできない。従って、1枚の光ディスクから多数のユーザがコンテンツのコピーを行う不正使用を防止することができる。

【0127】[コンテンツのコピー]次に、ユーザは、このコンテンツキー(Content-Key)を取得することで、光ディスクに登録されているコンテンツをHDD2にコピーすることが可能となる。

【0128】図9はこのコピー行程の流れを示すフローチャート、図10はこのコンテンツのコピーが行われる際に、クライアント端末装置1、HDD2及びメモリカード16の間で取り扱う情報を模式的に示した図である。この図9及び図10を用いてコンテンツのコピー行程の説明を行う。

【0129】まず、図9のフローチャートは、前述のメディアユニークIDの登録を終了し、コンテンツキーを

取得したユーザが、クライアント端末装置1を操作してコンテンツのコピーを指定することでスタートとなる。

【0130】ステップS21では、クライアント端末装置1のIOP32が、それぞれMC-Keyで暗号化されたコンテンツキー(Content-Key)及びコンテンツジェンキー(Content-Gen-Key)をメモリカード16から読み出し、これらをCPU30に供給する。

【0131】前述のように、MC-Keyは、システムサーバ装置4及びこのクライアント端末装置1でそれぞれ保持している。このため、CPU30は、この保持しているMC-Keyを用いて、上記暗号化されているコンテンツキー(Content-Key)及びコンテンツジェンキー(Content-Gen-Key)を復号化処理する。そして、CPU30は、この復号化したコンテンツキー及びコンテンツジェンキーをRAM36に記憶制御する。これにより、このコピー行程がステップS22に進む。

【0132】ステップS22では、IOP32が、コンテンツジェンキー(Content-Gen-Key)で暗号化されたクライアントID及びHDD-IDをメモリカード16から読み出し、これらをCPU30に供給する。CPU30は、先に復号化したコンテンツジェンキー(Content-Gen-Key)を用いてこのクライアントID及びHDD-IDを復号化する。

【0133】また、このステップS22では、CPU30が、上記復号化したクライアントIDと当該クライアント端末装置1に付されたクライアントIDとを照合する。また、CPU30は、上記復号化したHDD-IDと、当該クライアント端末装置1に接続されたHDD2のHDD-IDとを照合する。

【0134】次に、ステップS23では、CPU30が、上記各クライアントID、及び上記各HDD-IDがそれぞれ一致するか否かを判別する。両者が一致する場合はコンテンツのコピーを実行すべくこのコピー行程がステップS24に進む。両者が不一致の場合はこのコピー行程がステップS28に進む。

【0135】メモリカード16から復号化されたクライアントID及びHDD-IDが、そのクライアント端末装置1のクライアントID及びHDD-IDと一致しないということは、前述のコンテンツキー(Content-Key)の取得が、正規のユーザのクライアント端末装置1及びHDD2に基づいて行われていないことを示す。

【0136】すなわち、この場合、正規ユーザからメモリカード16を貸与された不正ユーザが、コンテンツのコピーを行おうとしていることを示している。

【0137】このため、CPU30は、例えば「コピーを行うことはできません。」等のコンテンツのコピーを拒否するメッセージをユーザに対して表示制御する。こ

れにより、中断されたかたちでこのコピー行程が終了することとなる。

【0138】次に、ステップS24は、クライアント端末装置1が、上記各クライアントID及び上記各HDD-IDの一致を検出した際に実行するステップである。この場合、CPU30は、光ディスク制御部33により光ディスクから再生されたコンテンツを、RAM36に記憶されているコンテンツキー（Content-Key）を用いて復号化する。また、CPU30は、この復号化したコンテンツを、RAM36に記憶されているコンテンツジェンキー（Content-Gen-Key）で再暗号化してHDD2に供給する。

【0139】次に、ステップS25では、HDD2が、図10に示すように上記コンテンツジェンキーで再暗号化されたコンテンツをハードディスクに保存（コピー）する。

【0140】次に、ステップS26ではクライアント端末装置1のCPU30がHDD2と通信を行うことで、コンテンツのコピーが完了したか否かを判別する。コピーが完了していない場合、CPU30は、前述のステップS24及びステップS25の動作を繰り返し実行制御することで、コンテンツのコピーが完了するまでの間、HDD2に対してコンテンツの供給を行う。コンテンツのコピーが完了すると、このコピー行程がステップS27に進む。

【0141】ステップS27では、コンテンツのコピーが完了したため、IOP32が、メモリカード16に記憶されているコンテンツキー（Content-Key）を消去する。これにより、このコピー行程が終了する。

【0142】このように、クライアント端末装置1は、コンテンツキー（Content-Key）で暗号化されて光ディスクに記憶されているコンテンツを、システムサーバ装置4から発行されたコンテンツキーで復号化してHDD2にコピーする。そして、このコンテンツのコピー後に、メモリカード16内に記憶されているコンテンツキー（システムサーバ装置4から発行されたコンテンツキー）を消去する。

【0143】前述のように、過去にコンテンツのコピーが行われた光ディスクに対しては、データベース3にコピー履歴が残るため、システムサーバ装置4は、原則的にコンテンツキーの再発行は行わない。このため、一度コンテンツのコピーが行われた光ディスクを貸与された第三者からのコピー申請は、システムサーバ装置4が、上記データベースのコピー履歴に基づいて拒否する。そして、システムサーバ装置4は、この第三者に対しては、コンテンツキーを送信しない。

【0144】上記第三者は、コンテンツキーを取得することができないため、貸与された光ディスクに記憶されているコンテンツを復号化することができない。このた

め、上記第三者がコンテンツをHDD等の二次記憶媒体にコピーすることができたとしても、コンテンツを復号化することができないことから、該コンテンツを使用することができない。従って、このコピー管理システムは、コンテンツの不正使用を防止することができる。

【0145】「コピーされたコンテンツの再生」次に、このようにHDD2にコピーされたコンテンツは、ユーザが繰り返し再生して利用することができるようになっている。

【0146】図11に、HDD2に保存されたコンテンツの再生行程の流れを示すフローチャートを示す。また、図12にこの再生行程において、クライアント端末装置1、HDD2及びメモリカード16の間で取り扱われる情報の模式図を示す。

【0147】図11のフローチャートは、前述のコンテンツのコピーを正規に終了させたユーザが、コンテンツの再生を指定することでスタートとなる。

【0148】ステップS31では、クライアント端末装置1のIOP32が、上記MC-Keyで暗号化されたコンテンツジェンキー（Content-Gen-Key）をメモリカード16から読み出し、これをCPU30に供給する。CPU30は、このコンテンツジェンキーを、クライアント端末装置1側で保持しているMC-Keyを用いて復号化して再生する。

【0149】次に、ステップS32では、IOP32が、コンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDをメモリカード16から読み出し、これをCPU30に供給する。CPU30は、先に復号化したコンテンツジェンキーを用いて、この暗号化されたクライアントID及びHDD-IDを復号化する。

【0150】次に、ステップS33では、CPU30が、当該クライアント端末装置1に付されているクライアントIDと、上記コンテンツジェンキーで復号化したクライアントIDとを照合する。

【0151】また、CPU30は、当該クライアント端末装置1に接続されているHDD2のHDD-IDと、上記コンテンツジェンキーで復号化したHDD-IDとを照合する。

【0152】上記各クライアントID及び上記各HDD-IDが一致しないということは、他のユーザのメモリカード16、他のユーザのクライアント端末装置1、或いは他のユーザのHDD2が用いられていることを示す。このため、CPU30は、ステップS35において、例えば「コンテンツを再生することはできません。」等のコンテンツの再生を拒否するメッセージをユーザに表示する。これにより、中断されるかたちでこのコンテンツの再生行程が終了することとなる。

【0153】このように、このコピー管理システムにおいては、HDD2にコピーされたコンテンツを再生する



際にも、クライアントID及びHDD-IDの照合を行う。例えば、正規のユーザが所有するメモリカード16とコンテンツが保存されたHDD2が、第三者に貸与された場合を考える。第三者は、自分のクライアント端末装置に対して、この貸与されたメモリカード16とHDD2を接続して、該HDD2内に記憶されているコンテンツの再生を行うこととなる。

【0154】しかし、メモリカード16内に記憶されているクライアントIDは、正規のユーザのクライアントIDである。このため、第三者のクライアント端末装置のクライアントIDと、メモリカード16に記憶されているクライアントIDとが一致しないことから、第三者のクライアント端末装置において、HDD2に記憶されているコンテンツの再生は拒否される。このため、メモリカード16とHDD2が貸与された場合でも、HDD2にコピーされているコンテンツの使用を防止することができる。

【0155】次に、上記各クライアントID及び上記各HDD2がそれぞれ一致した場合、CPU30は、先に復号化したコンテンツジェンキーを用いてHDD2のコンテンツを復号化し、これをRAM36に記憶する。これにより、このコンテンツの再生行程が終了する。

【0156】RAM36に記憶されたコンテンツが、例えばビデオゲームのゲームコンテンツであった場合、CPU30は、このゲームコンテンツに基づいて動作する。そして、CPU30は、例えばビデオゲームのキャラクタを表示制御し、効果音やBGM等を発音制御する。これにより、ユーザは、光ディスクからHDD2にコピーしたゲームコンテンツに基づいてビデオゲームを楽しむことができる。

【0157】光ディスクからゲームコンテンツを直接的に再生してビデオゲームを行う場合、新たなビデオゲームを行う毎に光ディスクの着脱作業が必要である。しかし、このように各光ディスクに記録されたゲームコンテンツをHDD2にコピーしておくことにより、新たなビデオゲームを行う毎に必要なとなっていた光ディスクの着脱作業を省略することができる。このため、新たなビデオゲームをスムーズに開始可能とすることができる。

【0158】なお、光ディスクからコンテンツのコピーが終了した後は、メモリカード16に記憶されているコンテンツキーが消去されるため、コンテンツの再コピーは行うことができない。しかし、メモリカード16に記憶されているコンテンツジェンキーは、コピー完了後も消去されることはない。このため、コンテンツジェンキーで暗号化されてHDD2にコピーされたコンテンツは、このメモリカード16に記憶されているコンテンツジェンキーを用いて繰り返し復号化して再生可能である。

【0159】〔デバイスの修理、交換に対する対応〕次に、このコピー管理システムの場合、システムサーバ装

置4は、クライアントID、HDD-ID、MC-ID等（以下、一括してデバイスIDという）と、ユーザIDとをユーザエントリ情報として一括して管理する。しかし、クライアント端末装置1やHDD2等のデバイスを破損等により交換した場合、この交換したデバイスのデバイスIDが、ユーザエントリ情報として登録されているデバイスIDとは異なるものとなる。従って、デバイスの交換を行うと、正規のユーザであるにも拘わらず、その交換したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【0160】一方、このコピー管理システムの場合、デバイスIDの固有性を確保することでコンテンツの不正使用を防止するようになっている。このため、クライアント端末装置1やHDD2等のデバイスを修理により復元した場合でも、この修理後のデバイスに対して、修理前に付されていたデバイスIDとは異なる新たなデバイスIDを付し、修理前のデバイスと修理後のデバイスとを明確に区別して管理することが好ましい。

【0161】ただ、このように修理後のデバイスに対して新たなデバイスIDを付すと、前述のデバイスの交換時と同様に、正規のユーザであるにも拘わらず、その修理したデバイスを用いてコンテンツのコピーや再生が不可能となることが懸念される。

【0162】このコピー管理システムは、デバイスの修理及び交換により新たなデバイスIDを用いることで懸念される上記不都合を、以下のように防止している。

【0163】〔クライアント端末装置及びHDDの修理、交換に対する対応〕図13に、このコピー管理システムにおけるクライアント端末装置及びHDDの修理、交換に対する対応を説明するための模式図を示す。この図13中、×印が描かれているクライアント端末装置1或いはHDD2は、破損したデバイスを示している。

【0164】この図13において、デバイスが破損した場合、ユーザは、その破損したデバイスを、メモリカード16と共に、このコピー管理システムを管理する管理者側のリペアセンターに送付する。

【0165】すなわち、この場合メモリカード16は破損していないのであるが、メモリカード16にはコンテンツジェンキー（Content-Gen-Key）やコンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-ID（以下、各IDを一括してデバイスIDという）が記憶されている。このため、デバイスが破損した場合でも、この破損したデバイスと共にメモリカード16を上記リペアセンターに送付（或いは持ち込み）するようになっている。

【0166】リペアセンターでは、故障したデバイスが送付されると、このデバイスが正常に動作するように修理、交換等すると共に、この修理、交換等したデバイスに対して新たなデバイスIDを付与する。

【0167】具体的には、クライアント端末装置1のクライアントIDは、例えば上記ハードウェアIDやオペレーティングシステムプログラムと共にMASK-ROM35に記憶されている。また、HDD2内にも上記MASK-ROM35と同様のMASK-ROMが設けられており、HDD-IDは、このMASK-ROMに記憶されている。このため、リペアセンターでは、デバイスの修理を行った場合には、この修理を行う前に設けられていたMASK-ROMを取り外し、新たなクライアントID或いはHDD-IDが記憶されたMASK-ROMに交換することで、新たなクライアントID或いはHDD-IDの付与を行う。

【0168】なお、デバイス自体を新品のデバイスに交換する場合は、この新品のデバイスのMASK-ROM内に、故障したデバイスとは異なるデバイスIDが記憶されているため、上記修理時のようなMASK-ROMの交換は行わない。

【0169】次に、リペアセンターのオペレータは、故障したデバイスと共に送付されたメモリカード16のMC-IDを再生する。オペレータは、リペアセンターに設けられている端末装置を介して上記システムサーバ装置4のデータベース3にアクセスし、上記メモリカード16から再生したMC-IDに基づいて、上記データベース3に記憶されているユーザエントリ情報を参照する。そして、オペレータは、端末装置を操作して、このデータベース3に記憶されているユーザエントリ情報のうち、デバイスIDを、新たに付与したデバイスIDに修正登録する。また、オペレータは、端末装置を介してデータベース3を操作し、コピー済みのコンテンツに対して立てられている上記フラグを降ろす。

【0170】また、オペレータは、端末装置を操作して、メモリカード16内に記憶されている、MC-Keyで暗号化されたコンテンツジェンキー(Content-Gen-Key)と、コンテンツジェンキー(Content-Gen-Key)で暗号化されたデバイスID(クライアントID及びHDD-ID)とをそれぞれ消去する。そして、このメモリカード16を、修理、交換等したデバイスと共にユーザに返送(或いは手渡し)する。

【0171】これにより、ユーザのデバイス(クライアント端末装置1、HDD2及びメモリカード16)の状態は、図5及び図6を用いて説明したユーザ登録行程が終了した直後の状態(=コンテンツのコピーを行う直前の状態)に戻るようになる。

【0172】このメモリカード16とデバイスが返送されたユーザは、図7及び図8を用いて説明したメディアユニークID(MID)の登録とコンテンツキー(Content-Key)の取得を再度行うようにクライアント端末装置1を操作する。

【0173】クライアント端末装置1は、ユーザの操作

に対応してシステムサーバ装置4にアクセスし、メディアユニークID(MID)の登録を行う。そして、クライアント端末装置1は、この登録によりシステムサーバ装置4から取得したコンテンツキー(Content-Key)を用いて光ディスクに記憶されているコンテンツをHDD2に再コピーする。

【0174】これにより、デバイスの修理や交換によりデバイスIDを新たに付与した場合でも、正規のユーザであれば、新たなデバイスIDに基づいてコンテンツのコピーや再生を実行可能とすることができる。

【0175】また、コピー管理システム側では、修理や交換により復元したデバイスに対して新たなデバイスIDを付すことにより、修理前のデバイスと修理後のデバイスとを明確に区別して管理することができる。

【0176】〔メモ리카ードの破損、紛失に対する対応〕次に、このコピー管理システムの場合、メモ리카ード16の破損、或いは紛失に対しては、以下のように対処する。図14に、このコピー管理システムにおけるメモ리카ード16の破損、紛失に対する対応を説明するための模式図を示す。この図14中、点線の枠で囲んで示すメモ리카ード16が、破損或いは紛失したメモ리카ード16を示している。

【0177】メモ리카ード16が破損或いは紛失した場合、ユーザは、この図14に示すように、インターネット5を介してクライアント端末装置1をシステムサーバ装置4に接続し、システムサーバ装置4に対してメモ리카ードの再発行を申請する。

【0178】この申請がなされるとシステムサーバ装置4は、ユーザIDの入力画面データをクライアント端末装置1側に送信する。これにより、ユーザのクライアント端末装置1は、テレビジョン受像機18にユーザIDの入力画面を表示制御する。

【0179】ユーザは、この入力画面に対してユーザIDの入力を行う。しかし、この場合、メモ리카ード16が破損或いは紛失しているため、メモ리카ード16からユーザID(User ID)を読み出すことはできない。このため、ユーザは、ユーザIDが発行された際にメモ帳等へ書き写しておいたユーザIDを見て、ユーザIDの入力を行う。クライアント端末装置1は、この入力されたユーザIDをシステムサーバ装置4に送信する。

【0180】次にシステムサーバ装置4は、このユーザから送信されたユーザIDに対応するユーザエントリ情報をデータベース3から参照する。これにより、システムサーバ装置4は、破損或いは紛失したメモ리카ード16のMC-ID及びMC-Keyと共に、コンテンツジェンキー(Content-Gen-Key)やそのメモ리카ード16でコピーされたコンテンツ等を認識することができる。

【0181】次に、システムサーバ装置4は、新たなM

C-IDを有するメモリカード16newに対して、新たなMC-Key (New-MC-Key) と、このNew-MC-Key で新たに暗号化したコンテンツジェンキー (Content-Gen-Key) と、このコンテンツジェンキー (Content-Gen-Key) で暗号化したクライアントID及びHDD-IDを記録し直す。また、システムサーバ装置4は、データベース3に記憶されているユーザエントリ情報が、この新たなメモリカード16Newに対応したユーザエントリ情報となるように、MC-IDやMC-Key等の書き換えを行う。

【0182】なお、この場合、メモリカード16が破損或いは紛失した場合であり、ユーザのクライアント端末装置1及びHDD2は正常に動作している。このため、コンテンツジェンキー (Content-Gen-Key) で暗号化されるクライアントID及びHDD-IDとしては、元のデバイスIDがそのまま用いられる。

【0183】次に、リペアセンターは、このメモリカード16newを、例えば郵送等によりユーザ側に物理的に送付する。前述のように、システムサーバ装置4側ではこのメモリカード16new内の各情報の書き換えと共に、データベース3のユーザエントリ情報の書き換えを行っている。このため、送付されたメモリカード16newを受け取ったユーザは、このメモリカード16new、クライアント端末装置1及びHDD2の組み合わせのシステムを用いて、以前と同様に、コンテンツのコピーや、コピーしたコンテンツの再生等を行うことができる。

【0184】〔第1の実施の形態の効果〕以上の説明から明らかなように、この第1の実施の形態のコピー管理システムは、システム管理者が、コンテンツキーで暗号化処理を施したコンテンツを、メディアユニークID

(MID) が付された光ディスクに記憶させてユーザに配布する。

【0185】ユーザは、コンテンツのコピーを行う際に、システムサーバ装置4に対して光ディスクのMIDを送信する。また、ユーザは、自分が使用しているデバイスのデバイスID (クライアントID、HDD-ID、MC-ID等) をシステムサーバ装置4に送信する。

【0186】システムサーバ装置4は、各ユーザが使用しているデバイスのデバイスIDに関連付けて、過去にコンテンツのコピーが行われた光ディスクのMIDをデータベース3に記憶している。

【0187】システムサーバ装置4は、ユーザからコンテンツのコピー申請がなされた際に、ユーザが使用しているデバイスIDと光ディスクのMIDに基づいてデータベース3を参照する。システムサーバ装置4は、データベース3内に同じMIDが登録されていないことを条件として、コンテンツを復号化するためのコンテンツキー

を、ユーザのクライアント端末装置1に送信する。

【0188】クライアント端末装置1は、このコンテンツキーを用いて光ディスクに記憶されているコンテンツを復号化してHDD2にコピーする。

【0189】このコピー管理システムは、データベース3内に登録されているMIDと同じMIDを掲示してコピー申請がなされた場合は、上記コンテンツキーの配信は行われぬ。このため、このコピー管理システムは、コンテンツのコピーを1回に制限することができ、コンテンツの不正コピーを防止することができる。

【0190】〔第2の実施の形態〕次に本発明の第2の実施の形態となるコピー管理システムの説明をする。上述の第1の実施の形態のコピー管理システムは、ユーザが自分のクライアント端末装置1をシステム管理者側のシステムサーバ装置4に直接的に接続してユーザ登録を行い、コンテンツキー (Content-Key) 等を取得してコンテンツのコピーを行うものであった。

【0191】この第2の実施の形態のコピー管理システムは、ユーザのクライアント端末装置1とシステム管理者側のシステムサーバ装置4との間に、第3者が管理する第3者管理サーバ装置が設けられている。ユーザはこの第3者管理サーバ装置を介してコンテンツキー (Content-Key) 等の取得を行う。第3者管理サーバ装置は、このコンテンツキー (Content-Key) 等の提供に対する課金を行う。

【0192】〔第2の実施の形態の構成〕図15に、この第2の実施の形態となるコピー管理システムのシステム構成図を示す。この図15は、光ディスクからコンテンツをコピーする際にコンテンツキー (Content-Key) を取得する流れを示している。

【0193】この図15において、システムサーバ装置4と第3者管理サーバ装置50とは、例えば専用回線や、公衆回線を専用回線のように利用可能なVPN (Virtual Private Network) 等により相互に接続されている。

【0194】また、システムサーバ装置4はインターネット5には接続されておらず、この第3者管理サーバ装置50がインターネット5に接続されている。このため、ユーザは、システムサーバ装置4に対して直接的にアクセスすることはできず、この第3者管理サーバ装置50を介して間接的にシステムサーバ装置4にアクセスすることとなる。

【0195】〔第2の実施の形態の動作〕次に、この第2の実施の形態のコピー管理システムの動作説明をする。この第2の実施の形態のコピー管理システムの場合、光ディスクからコンテンツのコピーを行おうとするユーザは、インターネット5を介して自分のクライアント端末装置1を第3者管理サーバ装置50に接続する。そして、ユーザは、クライアント端末装置1を介して、MC-ID、ユーザID (User ID)、メディア

ユニークID (MID) を第3者管理サーバ装置50側に送信する。また、ユーザは、クライアント端末装置1を介して、第3者管理サーバ装置50用のアカウント情報 (例えばユーザ名やパスワード等) を第3者管理サーバ装置50に送信する。

【0196】クライアント端末装置1は、MC-ID及びアカウント情報をそのまま第3者管理サーバ装置50に送信する。また、クライアント端末装置1は、ユーザID (User ID) 及び光ディスクのメディアユニークID (MID) をMC-Keyで暗号化し、これらを第3者管理サーバ装置50に送信する。

【0197】第3者管理サーバ装置50は、クライアント端末装置1から送信された各情報のうち、アカウント情報を抽出して取得する。また、第3者管理サーバ装置50は、専用回線 (或いは上記VPN) を介してMC-ID、MC-Keyで暗号化されたユーザID (User ID)、及びMC-Keyで暗号化されたメディアユニークID (MID) をシステムサーバ装置4に送信する。

【0198】システムサーバ装置4は、このMC-ID、ユーザID及びMIDを受信すると、前述と同様に暗号化されて光ディスクに記録されているコンテンツを復号化するためのコンテンツキー (Content-Key) をMC-Keyで暗号化して第3者管理サーバ装置50に返信する。また、システムサーバ装置4は、コンテンツジェンキー (Content-Gen-Key) をMC-Keyで暗号化して第3者管理サーバ装置50に返信する。さらにシステムサーバ装置4は、このコンテンツジェンキー (Content-Gen-Key) でユーザのクライアントID及びHDD-IDを暗号化して第3者管理サーバ装置50に返信する。

【0199】第3者管理サーバ装置50は、このMC-Keyで暗号化されたコンテンツキー (Content-Key)、MC-Keyで暗号化されたコンテンツジェンキー (Content-Gen-Key)、及びコンテンツジェンキー (Content-Gen-Key) で暗号化されたユーザのクライアントID、HDD-IDを、それぞれインターネット5を介してユーザのクライアント端末装置1に転送する。

【0200】第3者管理サーバ装置50は、コンテンツキー (Content-Key) を提供した代償として、先にクライアント端末装置1から送信された第3者管理サーバ装置50用のアカウント情報に基づいて、そのユーザに対する課金を行う。

【0201】クライアント端末装置1は、第3者管理サーバ装置50から送信された上記コンテンツキー、コンテンツジェンキー、クライアントID、及びHDD-IDをメモリカード16に記憶制御して、前述のようにコンテンツのコピー、及びコピーしたコンテンツの再生に用いる。

【0202】第3者管理サーバ装置50側には、例えばユーザのクレジットカードの番号や、プリペイドされた金額情報が予め登録されている。このため、第3者管理サーバ装置50は、コンテンツキーの提供と引き替えに課金した金額をクレジットカード会社に請求して回収する。或いは第3者管理サーバ装置50は、プリペイドされている残金から課金分の金額を減算して回収する。

【0203】このように回収された金銭は、例えばシステムサーバ装置4の管理者と第3者管理サーバ装置50の管理者との間において、所定の割合で分配されることとなる。

【0204】〔第2の実施の形態の効果〕このようにこの第2の実施の形態のコピー管理システムは、クライアント端末装置1とシステムサーバ装置4との間に第3者管理サーバ装置50を設けて構成する。ユーザはこの第3者管理サーバ装置50を介してシステムサーバ装置4にアクセスしてコンテンツキー (Content-Key) の配布を請求する。第3者管理サーバ装置50は、このコンテンツキー (Content-Key) をユーザに配布して課金を行う。

【0205】これにより、このコピー管理システムは、第3者 (第3者管理サーバ装置50の管理者) が介在するコピー管理システムという新規なコピー管理システムを提供することができる他、上述の第1の実施の形態のコピー管理システムと同じ効果を得ることができる。

【0206】また、このコピー管理システムは、コンテンツキーをユーザに配布した際に課金を行うことで、光ディスク等を介して、或いは所定のネットワークを介してコンテンツを無償でユーザに配布することができる。

【0207】なお、このコピー管理システムにおいて、光ディスクにMIDを付すことなくユーザに配布し、ユーザからコピーの申請があった際に、システムサーバ装置4或いは第3者管理サーバ装置50が、そのユーザに対してコンテンツキーを配布して課金を行うようにしてもよい。

【0208】また、この第2の実施の形態のコピー管理システムは、第3者管理サーバ装置50が課金を行うこととしたが、これは、システムサーバ装置4が課金を行うようにしてもよい。

【0209】最後に、本発明は一例として説明した上述の各実施の形態に限定されることはない。このため、上述の各実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論である。

【0210】例えば、上述の各実施の形態の説明では、クライアント端末装置1は、デバイス識別情報として、クライアントID、HDD-ID及びMC-IDをシステムサーバ装置4に送信することとした。しかし、クライアント端末装置1からクライアントIDのみをシステムサーバ装置4に送信してもよい。同様に、クライアン

ト端末装置 1 から HDD-ID のみをシステムサーバ装置 4 に送信してもよい。同様に、クライアント端末装置 1 から MC-ID のみをシステムサーバ装置 4 に送信してもよい。

【0211】また、クライアント端末装置 1 からクライアント ID 及び HDD-ID をシステムサーバ装置 4 に送信してもよい。同様に、クライアント端末装置 1 からクライアント ID 及び MC-ID をシステムサーバ装置 4 に送信してもよい。同様に、クライアント端末装置 1 から HDD-ID 及び MC-ID をシステムサーバ装置 4 に送信してもよい。

【0212】すなわち、上述の各実施の形態のコピー管理システムは、システムサーバ装置 4 側で、コンテンツのコピーが行われる記憶媒体と、コンテンツのコピーに使用されるデバイスとを関連付けてコピー管理を行うことで不正コピーを防止する。このため、クライアント端末装置 1 からシステムサーバ装置 4 に送信されるデバイス識別情報としては、ユーザを特定可能な識別情報であればよい。

【0213】また、上述の各実施の形態の説明では、メモリカード 16 を用いることとしたが、このコピー管理システムの場合、必ずしもメモリカード 16 は必要としない。メモリカード 16 を用いない場合は、メモリカード 16 に記憶される上記コンテンツキーやコンテンツジェンキー等は、HDD 2 やクライアント端末装置 1 に内蔵されているメモリに記憶させればよい。

#### 【0214】

【発明の効果】本発明は、記憶媒体の持ち主である正規のユーザに対してのみ、記憶媒体に記憶されたコンテンツのコピーを許可することができる。このため、記憶媒体に記憶されたコンテンツの不正コピーを防止することができる。

#### 【図面の簡単な説明】

【図 1】本発明の第 1 の実施の形態のコピー管理システムのシステム構成を示すブロック図である。

【図 2】コピー管理システムを構成するクライアント端末装置及びハードディスクドライブ (HDD) の外観を示す斜視図である。

【図 3】クライアント端末装置の電気的な構成を示すブロック図である。

【図 4】コンテンツキー (Content-Key) で暗号化されたデジタルコンテンツが記憶された、このコピー管理システムに用いられる光ディスクを説明するた

めの図である。

【図 5】コピー管理システムにおけるユーザ登録の流れを示すフローチャートである。

【図 6】ユーザ登録時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

【図 7】コピー管理システムにおける、光ディスクに個別に付されたメディアユニーク ID (MID) の登録動作と、コンテンツキー (Content-Key) の取得動作を示すフローチャートである。

【図 8】光ディスクに個別に付されたメディアユニーク ID (MID) の登録時、及びコンテンツキー (Content-Key) の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すコピー管理システムの模式図である。

【図 9】コピー管理システムにおけるコピー行程の流れを示すフローチャートである。

【図 10】コピー実行時にクライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される各情報を示す模式図である。

【図 11】コピー管理システムにおける、ハードディスクドライブにコピーしたデジタルコンテンツの再生動作を示すフローチャートである。

【図 12】ハードディスクドライブにコピーしたデジタルコンテンツの再生時に、クライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される情報を示す模式図である。

【図 13】クライアント端末装置或いはハードディスクドライブの修理或いは交換に対するコピー管理システムの対応を説明するための模式図である。

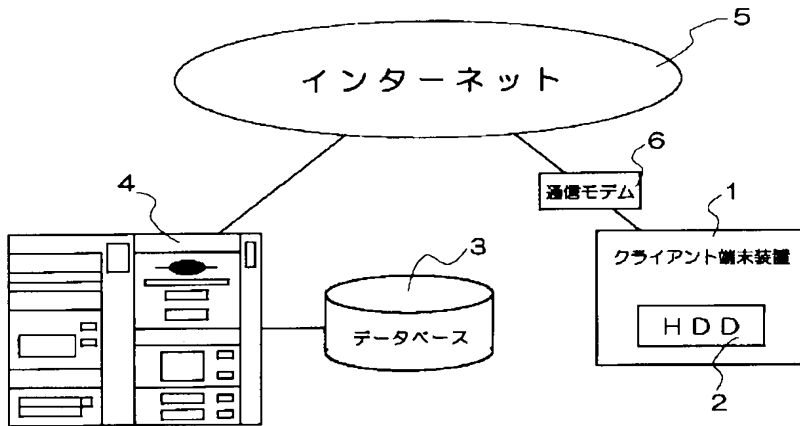
【図 14】メモリカードの破損或いは紛失に対するコピー管理システムの対応を説明するための模式図である。

【図 15】光ディスクに個別に付されたメディアユニーク ID (MID) の登録時、及びコンテンツキー (Content-Key) の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示す、本発明の第 2 の実施の形態となるコピー管理システムの模式図である。

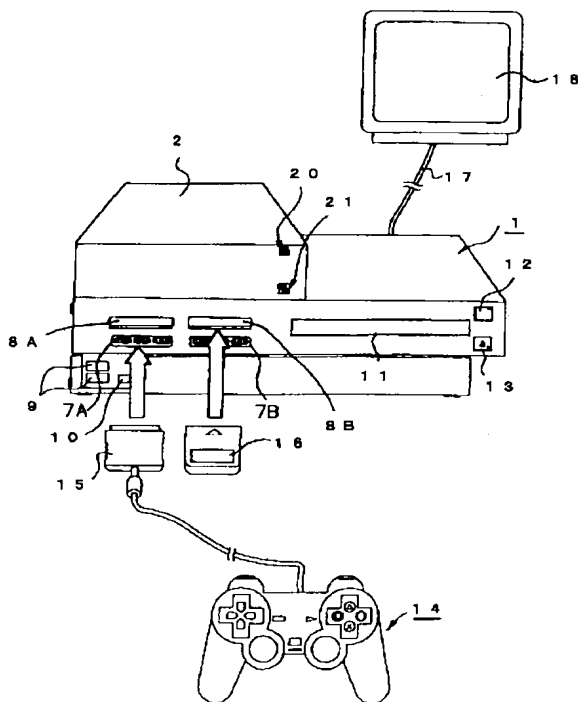
#### 【符号の説明】

1…クライアント端末装置、2…ハードディスクドライブ (HDD)、3…データベース、4…システムサーバ装置、5…インターネット、6…通信モデム

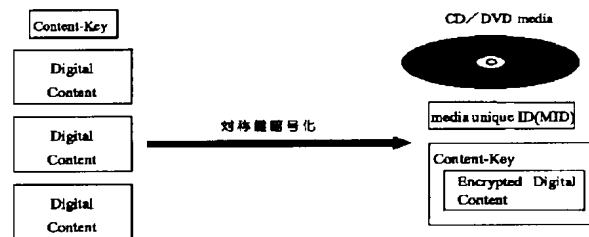
【図 1】



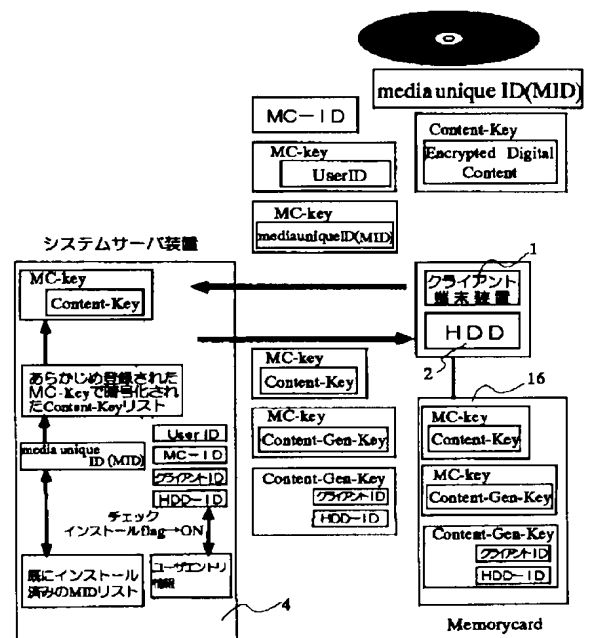
【図 2】



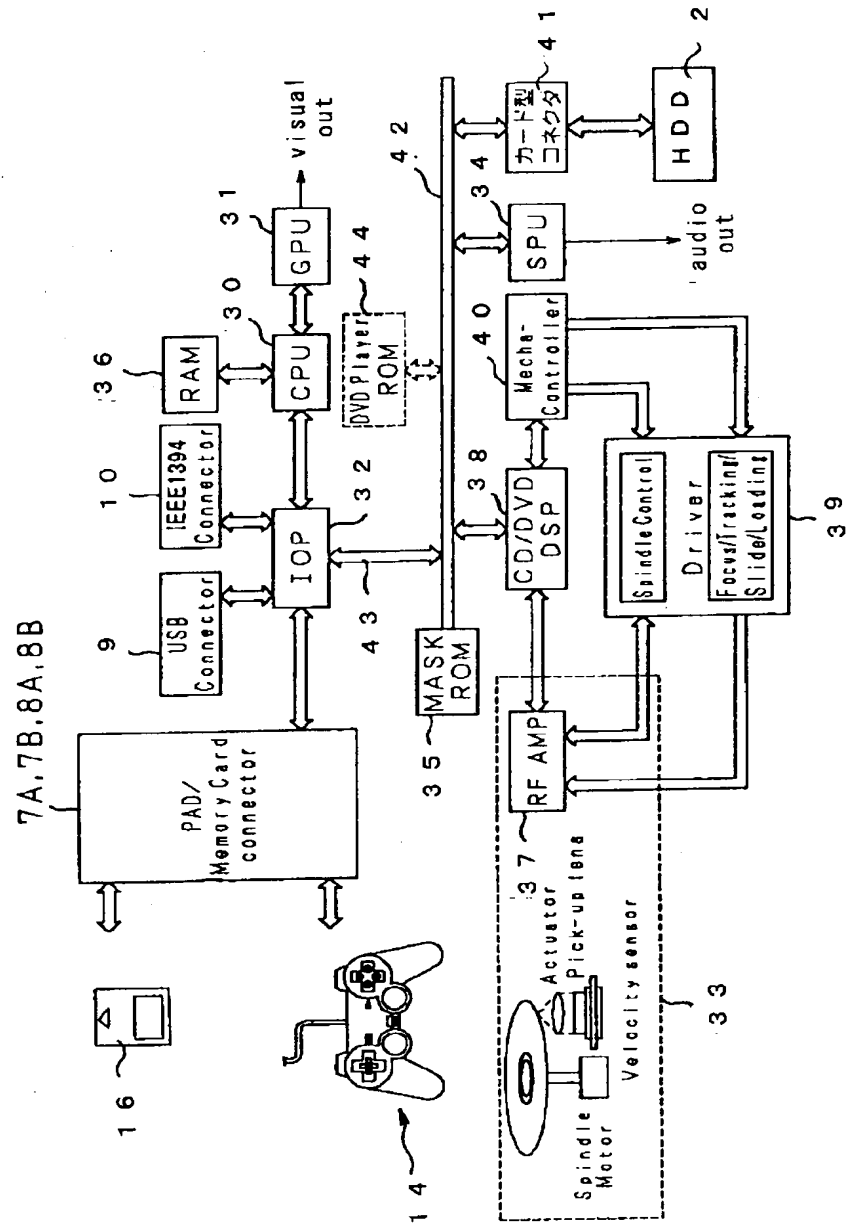
【図 4】



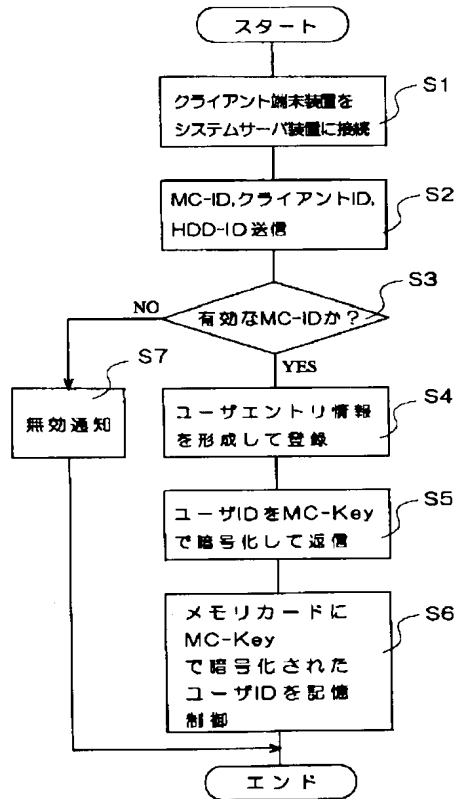
【図 8】



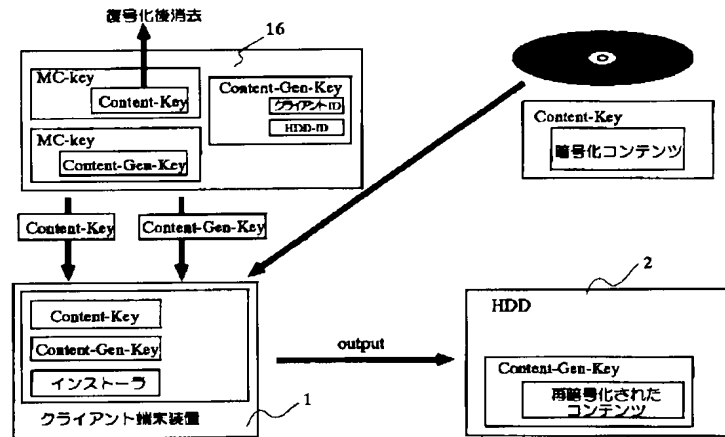
【図3】



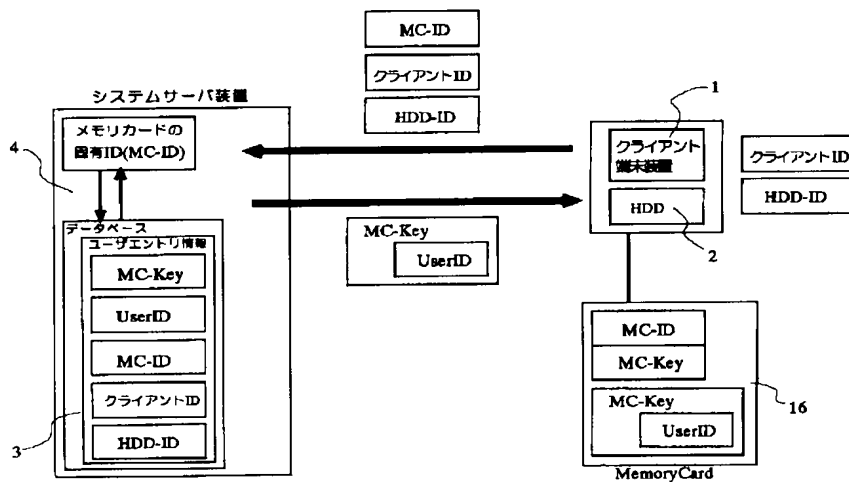
【図5】



【図10】

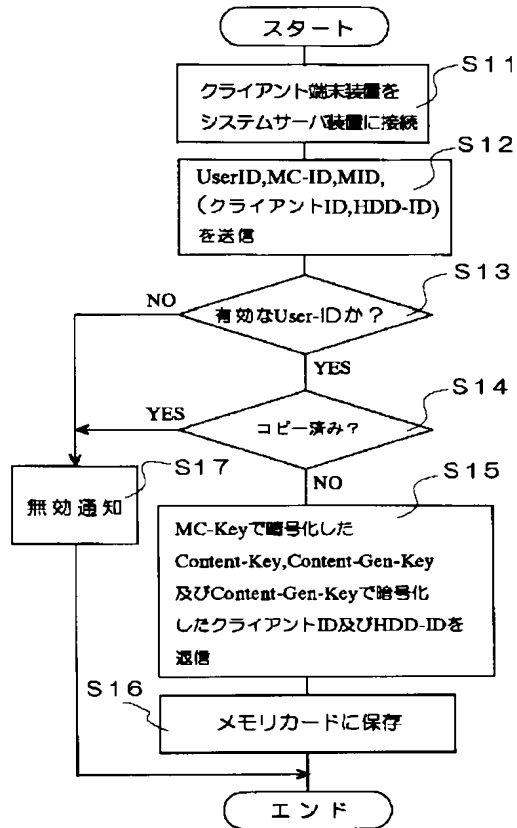


【図6】

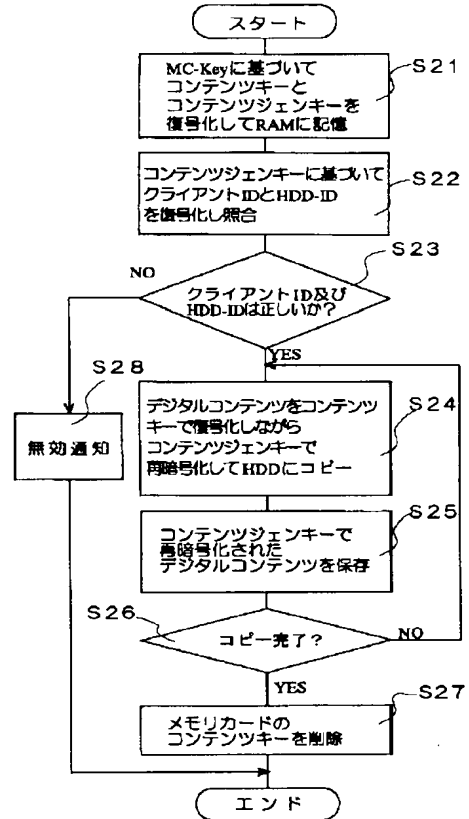




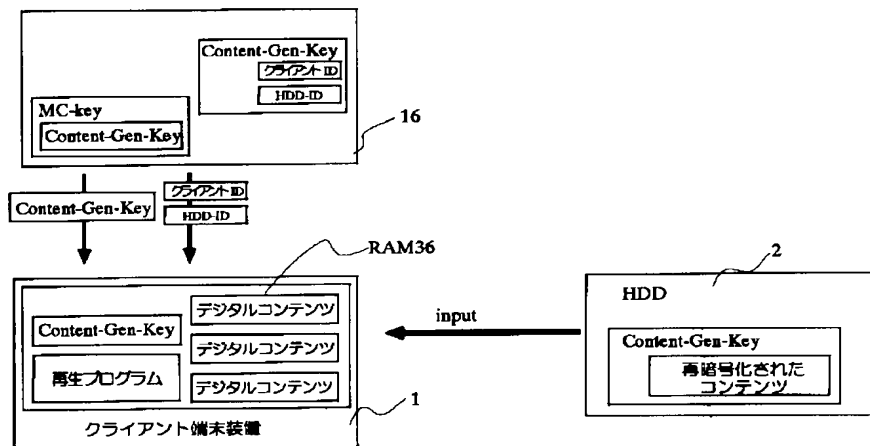
【図7】



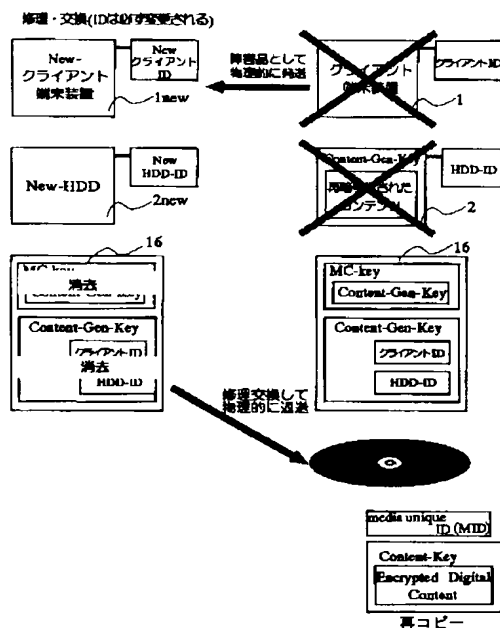
【図9】



【図12】



【图 1 3】



【图 1-4】

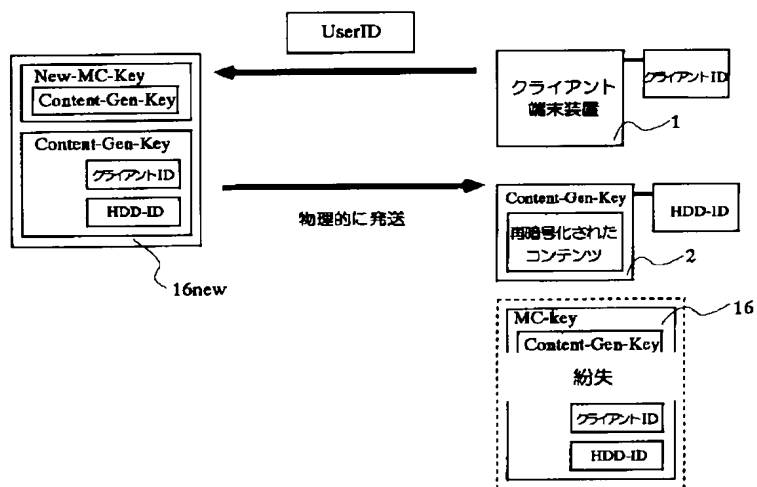


Figure 1 illustrates the system configuration. It shows three main components: a System Server Device (4), a Third Party Management Server Device (50), and a Client Device (1). The System Server Device (4) contains an MC-Key and Content-Key. The Third Party Management Server Device (50) contains an MC-Key, Content-Gen-Key, and a HDD-ID. The Client Device (1) contains a Client Device ID, a HDD, and a Content-Gen-Key. Data flows are indicated by arrows: from the System Server Device (4) to the Client Device (1) via the Content-Key, and from the Third Party Management Server Device (50) to the Client Device (1) via the Content-Gen-Key. The Client Device (1) also contains an MC-ID and a Content-Key. The Third Party Management Server Device (50) also contains an MC-ID and a Content-Key. The Client Device (1) also contains a Content-Gen-Key and a HDD-ID. The Third Party Management Server Device (50) also contains a Content-Gen-Key and a HDD-ID. The Client Device (1) also contains a Content-Gen-Key and a HDD-ID. The Third Party Management Server Device (50) also contains a Content-Gen-Key and a HDD-ID.

【請求項6】 請求項1から請求項5のうち、いずれか一項記載のコピー管理システムであって、

上記サーバ装置は、上記コピーするコンテンツを暗号化するための暗号化鍵を送信し、  
上記ユーザ端末装置は、上記コンテンツを上記暗号化鍵で暗号化して上記第 1 の記憶装置にコピーすると共に、  
上記暗号化鍵を所定の記憶手段に記憶し、該記憶手段に記憶した暗号化鍵を用いて、上記第 1 の記憶装置にコピーされたコンテンツを復号化して再生することを特徴とするコピー管理システム。

【請求項 7】 請求項 1 から請求項 6 のうち、いずれか一項記載のコピー管理システムであって、  
上記サーバ装置は、上記コピー許可情報の送信が終了した媒体識別情報を、各ユーザのユーザ端末装置に付されている装置識別情報に関連付けてデータベースに記憶し、修理或いは交換によりユーザ端末装置の識別情報が変更された場合、上記データベースに登録されている装置識別情報を、変更された装置識別情報に書き換えることを特徴とするコピー管理システム。

【請求項 8】 請求項 1 から請求項 7 のうち、いずれか一項記載のコピー管理システムであって、  
上記サーバ装置は、上記コピー許可情報の送信を行ったユーザ端末装置を有するユーザに対して所定の課金処理を行うことを特徴とするコピー管理システム。

【請求項 9】 請求項 1 から請求項 8 のうち、いずれか一項記載のコピー管理システムであって、  
上記ユーザ端末装置と上記サーバ装置との間で情報の送受信を仲介すると共に、少なくとも上記コピー許可情報をユーザ端末装置に送信した際に、該ユーザに対する課金処理を行う仲介サーバ装置を有することを特徴とするコピー管理システム。

【請求項 10】 記憶されている所定のコンテンツ及び固有の媒体識別情報のうち、該媒体識別情報を読み出すステップと、  
ユーザが上記コンテンツのコピーを行う際に使用するユーザ端末装置を構成する装置に対して付された装置識別情報を読み出すステップと、  
少なくとも上記読み出した媒体識別情報及び装置識別情報を、所定のサーバ装置に送信するステップと、  
上記媒体識別情報及び装置識別情報を送信することで、上記サーバ装置から送信される、上記コンテンツのコピーを許可するコピー許可情報を受信するステップと、  
上記受信したコピー許可情報を用いて、上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第 1 の記憶装置にコピーするステップとを有するユーザ端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 11】 請求項 10 記載の記憶媒体であって、  
上記コピー許可情報は、上記送信した装置識別情報で暗号化されており、  
上記受信したコピー許可情報を、上記装置識別情報で復号化するステップを有することを特徴とする記憶媒体。

【請求項 12】 請求項 10 又は請求項 11 記載の記憶媒体であって、

上記コンテンツのコピー後に、上記コピー許可情報を削除するステップを有することを特徴とする記憶媒体。

【請求項 13】 請求項 10 から請求項 12 のうち、いずれか一項記載の記憶媒体であって、  
上記サーバ装置から送信される、上記コピーするコンテンツを暗号化するための暗号化鍵を受信するステップと、  
上記コンテンツを、上記暗号化鍵で暗号化してコピーするステップと、  
上記暗号化鍵を記憶手段に記憶するステップと、  
上記コピーされたコンテンツを再生する際に、上記記憶手段に記憶されている暗号化鍵を用いて上記コピーされたコンテンツを復号化して再生するステップとを有することを特徴とする記憶媒体。

【請求項 14】 請求項 10 から請求項 13 のうち、いずれか一項記載の記憶媒体であって、  
上記媒体識別情報及び装置識別情報を送信するステップでは、ユーザ端末装置本体に付された端末装置識別情報、上記第 1 の記憶装置に固有に付された第 1 の装置識別情報、及びユーザ端末装置を構成する第 2 の記憶装置に固有に付された第 2 の装置識別情報のうち、いずれか 1 つ或いは複数を組み合わせて上記装置識別情報として上記サーバ装置に送信することを特徴とする記憶媒体。

【請求項 15】 ユーザ端末装置から送信される、該ユーザ端末装置を構成する装置に付された装置識別情報、及び所定のコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、  
対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記受信した媒体識別情報が、上記受信した装置識別情報に関連付けされて登録されているか否かを検出するステップと、  
上記受信した媒体識別情報の未登録が検出された際に、上記受信した装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信するステップとを有するサーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【請求項 16】 所定のコンテンツが記憶されると共に、固有の媒体識別情報が付された記憶媒体から、該媒体識別情報を読み出すステップと、  
ユーザが上記コンテンツのコピーを行う際に使用するユーザ端末装置を構成する装置に対して付された装置識別情報を読み出すステップと、  
少なくとも上記読み出した媒体識別情報及び装置識別情報を、所定のサーバ装置に送信するステップと、  
上記媒体識別情報及び装置識別情報を送信することで、上記サーバ装置から送信される、上記コンテンツのコピー

一を許可するコピー許可情報を受信するステップと、上記受信したコピー許可情報を用いて、上記記憶媒体に記憶されているコンテンツを、ユーザ端末装置を構成する第1の記憶装置にコピーするステップとを有するユーザ端末装置の情報処理プログラム。

【請求項17】 ユーザ端末装置から送信される、該ユーザ端末装置を構成する装置に付された装置識別情報、及び所定のコンテンツが記憶された記憶媒体に対して固有に付された媒体識別情報を受信するステップと、対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記受信した媒体識別情報が、上記受信した装置識別情報に関連付けされて登録されているか否かを検出するステップと、上記受信した媒体識別情報の未登録が検出された際に、上記受信した装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可

情報を送信するステップとを有するサーバ装置の情報処理プログラム。

【請求項18】 固有の媒体識別情報が付された記憶媒体に記憶されているコンテンツのコピーを行う際に、該媒体識別情報と共に、ユーザ端末装置を構成する装置に付された装置識別情報を、該ユーザ端末装置からサーバ装置に送信し、上記サーバ装置において、対応する装置識別情報に関連付けされた状態で、コンテンツのコピーが行われた記憶媒体の媒体識別情報が登録されるデータベースから、上記送信された媒体識別情報が、上記送信された装置識別情報に関連付けされて登録されているか否かを検出し、上記データベースに、上記媒体識別情報が未登録であった場合に、上記サーバ装置から、上記送信された装置識別情報に対応するユーザ端末装置に対して、上記コンテンツのコピーを許可するコピー許可情報を送信するコピー管理方法。

#### フロントページの続き

(51) Int. Cl. 7		識別記号	F I	テーマコード (参考)	
G 0 6 F	17/60	5 1 2	G 0 6 F 17/60	5 1 2	
		Z E C		Z E C	
H 0 4 L	9/08		H 0 4 L 9/00	6 7 3 B	
	9/32			6 0 1 B	
(72)発明者	岡本 伸一		(72)発明者	島川 恵三	
	東京都港区赤坂7丁目1番1号 株式会社			東京都港区赤坂7丁目1番1号 株式会社	
	ソニー・コンピュータエンタテインメント			ソニー・コンピュータエンタテインメント	
	内			内	
(72)発明者	吉森 正治		(72)発明者	岡田 豊史	
	東京都港区赤坂7丁目1番1号 株式会社			東京都港区赤坂7丁目1番1号 株式会社	
	ソニー・コンピュータエンタテインメント			ソニー・コンピュータエンタテインメント	
	内			内	
(72)発明者	犬井 努		(72)発明者	九保 亮	
	東京都港区赤坂7丁目1番1号 株式会社			東京都港区赤坂7丁目1番1号 株式会社	
	ソニー・コンピュータエンタテインメント			ソニー・コンピュータエンタテインメント	
	内			内	
			(72)発明者	中村 光宏	
				東京都港区赤坂7丁目1番1号 株式会社	
				ソニー・コンピュータエンタテインメント	
				内	
			F ターム (参考)	5B017 AA06 BA05 BA07 CA15	
				5J104 AA07 AA13 KA02 PA14	

- (54) 【発明の名称】 コピー管理システム，クライアント端末装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，管理サーバ装置の情報処理プログラムが記憶されたコンピュータ読み取り可能な記憶媒体，クライアント端末装置の情報処理プログラム，管理サーバ装置の情報処理プログラム，コピー管理方法，クライアント端末装置の情報処理方法、及び管理サーバ装置の情報処理方法